#SHAREorg

SHARE
Technology · Connections · Results

Why Legacy Security Isn't Enough

Session #14228

Monday, August 12 at 11:00 am
Hynes Convention Center Room 207

Paul R. Robichaux

SHARE in Boston

Abstract and Speaker

- Information System Security, the freedom from loss and/or misuse of data and/or information services, and the System Professionals charged with protecting the zEnterprise are consistently under attack from an every evolving set of persistent external and internal threats and the often unintended consequences of threats that emerge from regulatory and/or technological changes.

- More likely then not, the tools and methods used to detect and defend against these mutating threats are inadequate, often out-of-date. Accepted reasons for this *"Risky State of Affairs"* supports only the status quo, none should be considered reasonable or acceptable.

- Failure to evolve our defenses and responses at a pace as fast or faster then the threats they defend against places the integrity of the zEnterprise in an unacceptable state of risk.

- This presentation will provide insight into:

  First, How to use z/OS Comm Server Policy Based Management to defend against External Threats.

  Second, How to adapt ISPF Services to better Manage and Control Threats to z/OS Configurations.

  Third, How to use Xbridge and Vanguard Tools and Services to comply with regulatory requirements.

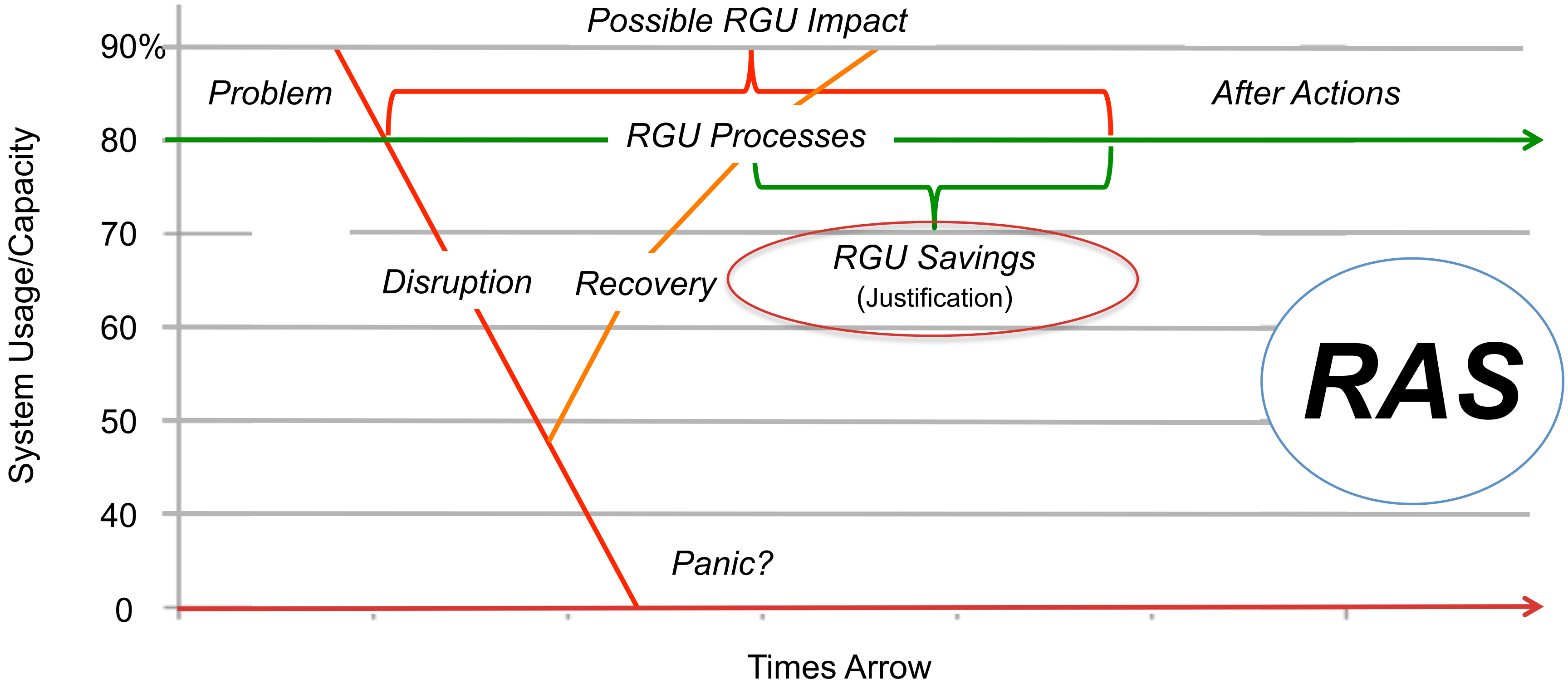
  Fourth, How to put the future of Information System Security into perspective.

- Paul R. Robichaux is CEO of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a Certified Public Accountant.

- The corporate mission of NewEra Software is to provide software solutions that help users avoid non-compliance, make corrections as needed and in doing so, continuously improve z/OS integrity.

Legacy Security?

Why an IBM Mainframe? > Most Reliable, Available, ~~Serviceable~~ *Securable*



RGU = Revenue Generating Unit

Legacy Security?

Why an IBM Mainframe? Lowest Total Cost of Ownership!

Industry	RGU*	Mainframe	Distributed	% Difference
Retail	*Location*	$ 421,346.000	$ 560,300.000	24.7 ↓
Auto	*Vehicle*	275.000	370.000	25.7 ↓
Banking[1]	*Transaction*	.120	.350	65.7 ↓
Web	*Click-Through*	.046	.041	12.2 ↑

* RGU = Revenue Generating Unit

[1] Of the World's 60 Largest Banks, 59 use Mainframes running z/OS

Source: Dr. John Shedletsky – IBM Technical World – Reporting on Gartner Group Findings

Legacy Security?

This is all about "How To"!

☑ Understand the "Real Threats" to zEnterprise Security

☑ Use the z/OS Comm Server to Defend against External Threats

☑ Adapt ISPF Services to Manage and Control Internal Threats to z/OS

☑ Mine for Data Exposures and Mitigate Risk Using Xbridge "*DATASNIFF*"

☑ Enforce zEnterprise Configuration Compliance with Vanguard

☑ How to put the future of Information System Security into Perspective

Legacy Security?

Real Threats to zEnterprise System Security! > The Real Threat!

The latest "Anecdotal Findings" are good news for people who like bad news:

"…there are more threats than there are people or tools to identify and resolve them."

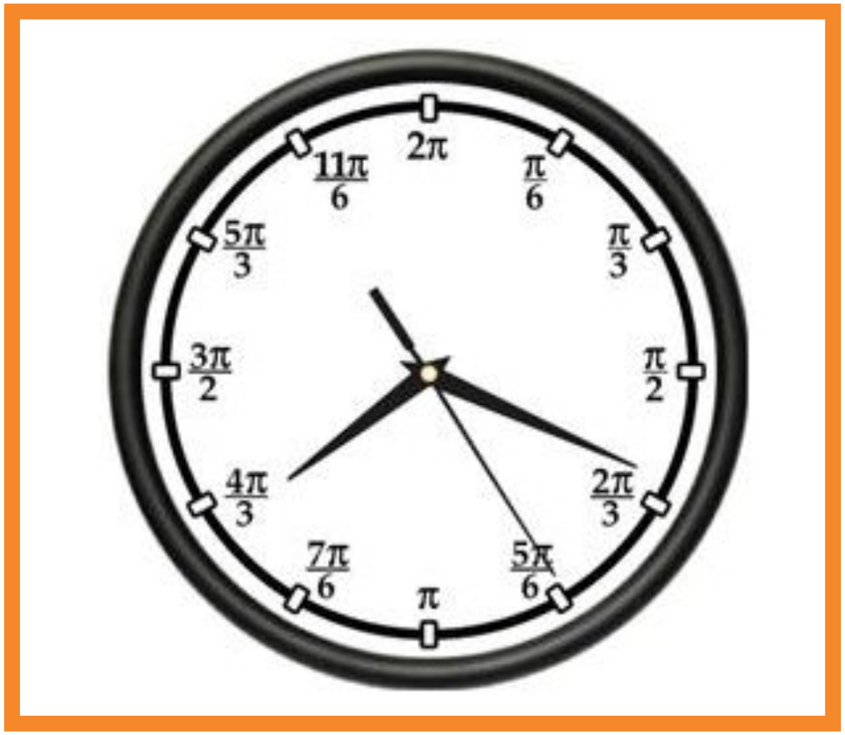
Legacy Security?

Real Threats to zEnterprise System Security! > The Real Threat!

☑ As with all things, time ages even the best concepts and designs. With this inevitability in mind today’s Security Professionals are facing threats that require agility in the application of security that cannot be easily implemented with Legacy Security.

☑ The application of Legacy Security within the broader base of users, applications and data resources is adequate and will continue, as is, into the foreseeable future.

☑ When the security needed to protect zEnterprise System configurations and resources is considered, it becomes clear that we are rapidly approaching a state of non-compliance.



Legacy Security?

Real Threats to zEnterprise System Security! > The Real Threat!

☑ *Explosion in External Threats*

Commodity Threats
Advanced Persistent Threats
Coordinated Actions/Activities

☑ *Graying of Security Assets*

Resulting from Retirements, Reductions in Workforce and a Misguided Emphasis on Non-Mainframe platforms.

☑ *Flood of System Messages*

Driven primarily by advances in Hardware, they are now generated at a rate 1200 X faster than 15 years ago.

☑ *Reliance on Consultants/Outsourcers*

Often seen as a strategy for reducing cost, these dependencies move control into the hands of others.

☑ *Drive Towards Globalization*

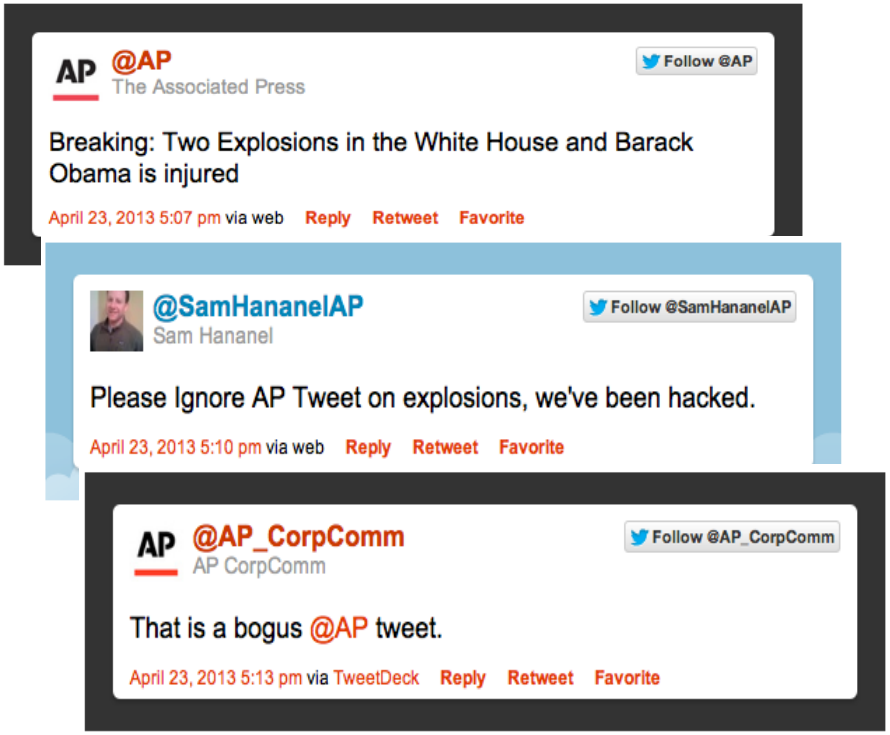
Different cultures will view security in ways that conform to their view of best practices.

☑ *"Starving the Beast"*

A myopic focus on the Total Cost of Ownership will result in a diminished view of the value of information security.

Legacy Security?

Real Threats to zEnterprise System Security! > The Real Threat!



AP **@AP** The Associated Press — Follow @AP

Breaking: Two Explosions in the White House and Barack Obama is injured

April 23, 2013 5:07 pm via web Reply Retweet Favorite

@SamHananelAP Sam Hananel — Follow @SamHananelAP

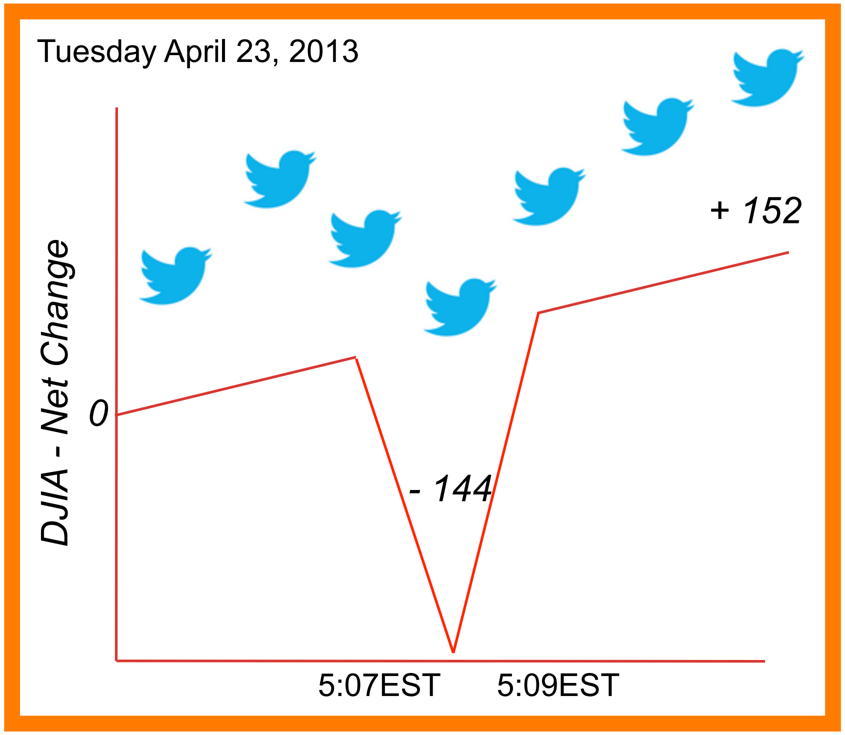
Please Ignore AP Tweet on explosions, we've been hacked.

April 23, 2013 5:10 pm via web Reply Retweet Favorite

AP **@AP_CorpComm** AP CorpComm — Follow @AP_CorpComm

That is a bogus @AP tweet.

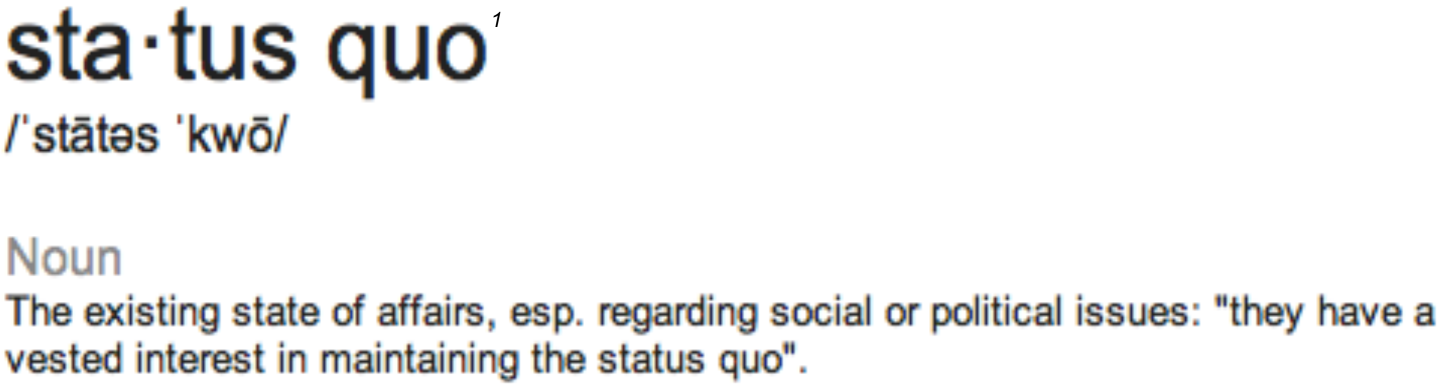
April 23, 2013 5:13 pm via TweetDeck Reply Retweet Favorite



Source:http://www.huffingtonpost.com/2013/04/23/ap-twitter-hacked_n_3140277.html

Legacy Security?

Real Threats to zEnterprise System Security! > What? Me Worry!



sta·tus quo[1]

/ˈstātəs ˈkwō/

Noun

The existing state of affairs, esp. regarding social or political issues: "they have a vested interest in maintaining the status quo".

[1] *Source: http://en.wikipedia.org/wiki/status_quo*

Legacy Security?

We're all under Attack! Has Your Mainframe has be Compromised?

"…In Q4/2012 more than 8 million new kinds of malware were discovered, up 25% from the prior years. There are now more than 90 million unique strands of malware in the wild."

Source: "Threats Report" by McAfee an Intel subsidiary

"…of the 3,236 US Businesses asked, 43% reported data lost in a Public or Private Cloud."

Source: San Jose Mercury - Symantec Corp. - March, 2013

"…In 2012 Security Breaches Cost US Companies an Estimated $US175 Billion."

Source: The Ponemon Institute – www.ponemon.org an Annual Survey 2012

Legacy Security?

We're all under Attack! > Attack Types to Defend Against > More!

☑ Advanced Persistent Threat:

A Who not a What!

"Comment Crew" - "Shanghai Group" - "APA 1"

☑ Commodity Threat:

More a What than a Who!

"Phishing", "Scanning"

☑ Embedded:

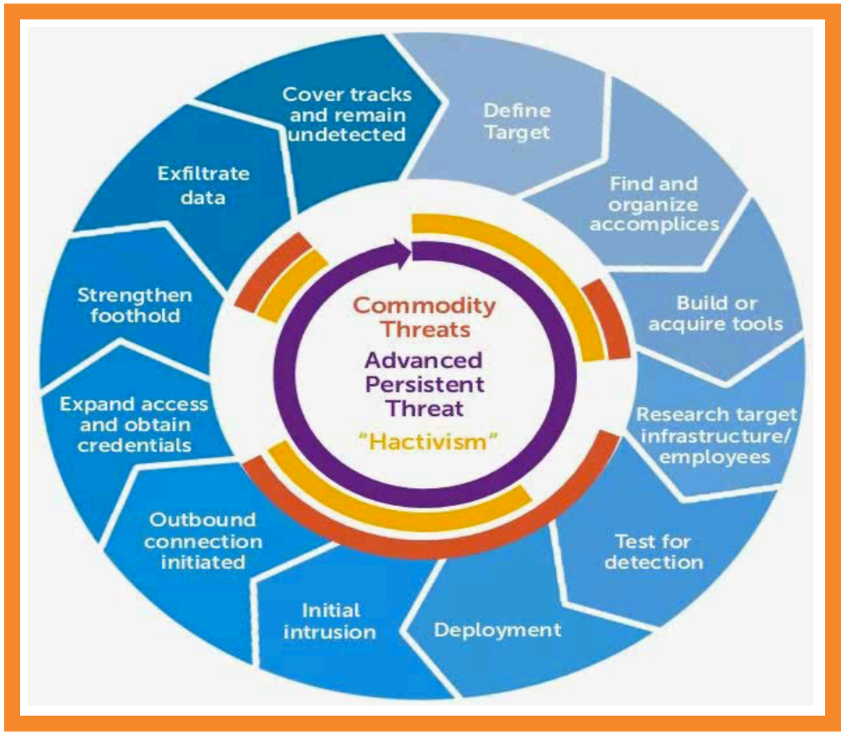
Comes with the Platform!

"Huawei inspires fear", "It's me"

☑ Legislated:

The Government Says It's OK!

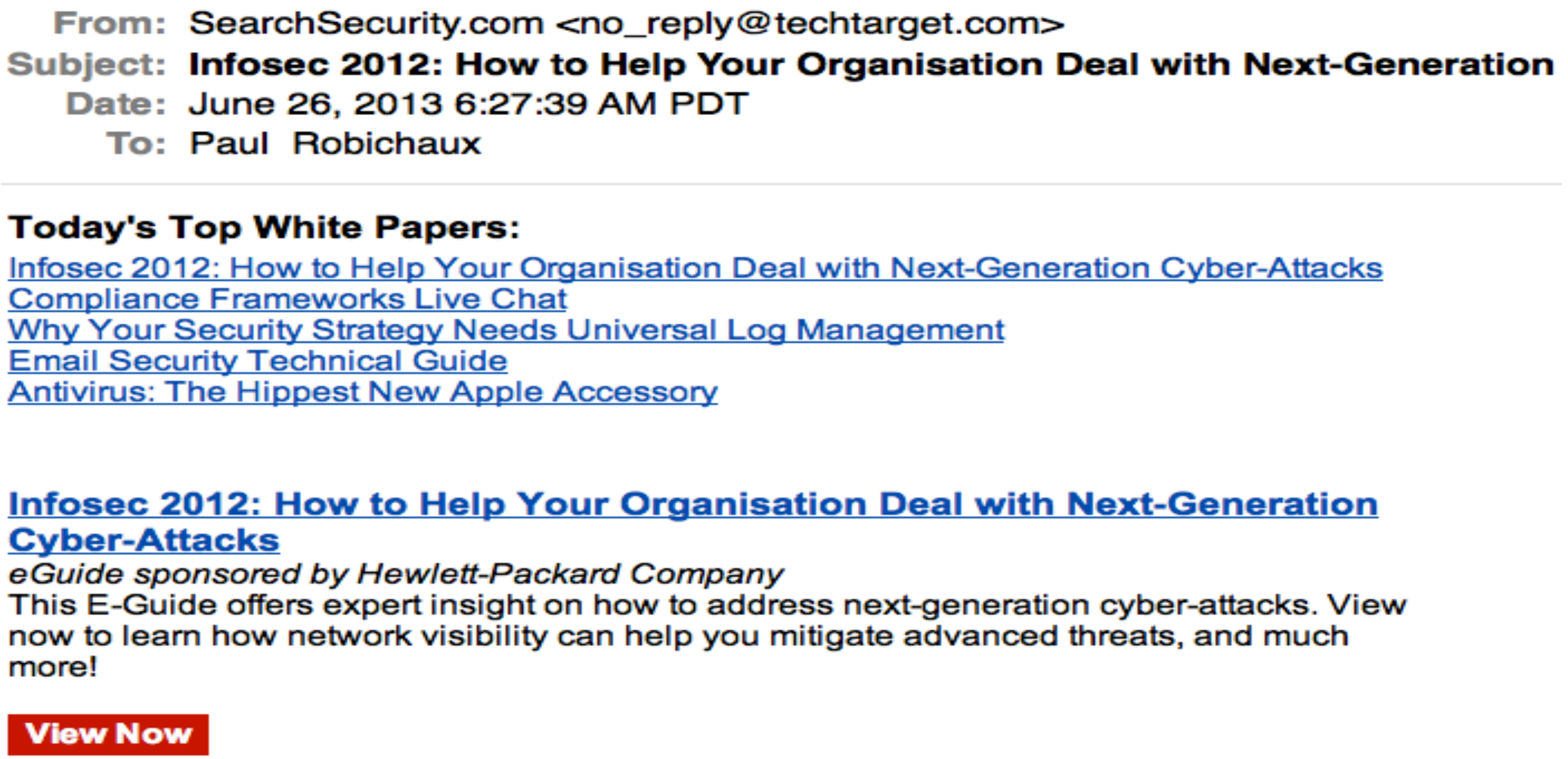
"Market takes a Flash Crash"


Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Source: Anatomy of an Advanced Persistent Threat - A Webcast - Dell SecureWorks - Posted 02.03.2012
http://en.wikipedia.org/wiki/Phishing

Legacy Security?

We're all under Attack! > Best Defense Common Sense > Awareness!



From: SearchSecurity.com <no_reply@techtarget.com>
Subject: **Infosec 2012: How to Help Your Organisation Deal with Next-Generation**
Date: June 26, 2013 6:27:39 AM PDT
To: Paul Robichaux

Today's Top White Papers:

Infosec 2012: How to Help Your Organisation Deal with Next-Generation Cyber-Attacks
Compliance Frameworks Live Chat
Why Your Security Strategy Needs Universal Log Management
Email Security Technical Guide
Antivirus: The Hippest New Apple Accessory

Infosec 2012: How to Help Your Organisation Deal with Next-Generation Cyber-Attacks
eGuide sponsored by Hewlett-Packard Company
This E-Guide offers expert insight on how to address next-generation cyber-attacks. View now to learn how network visibility can help you mitigate advanced threats, and much more!

Source: Techtarget - http://www.techtarget.com/

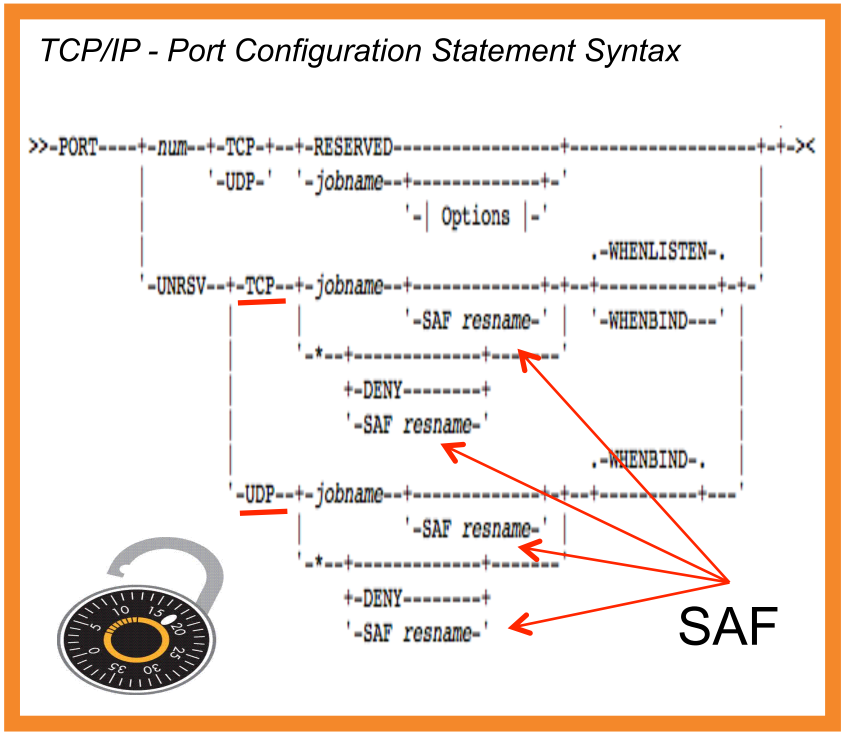
Legacy Security?

We're all under Attack! > Use What is Currently Available > SAF

☑ The PORT statement is used to reserve a port for one/more job names or to control application access to unreserved ports.

☑ For example, use the PORT statement to control the port that will be used by the SMTP server for receiving mail. If PORT is not coded, SMTP defaults to the value 25, the well known port for mail service.

☑ Note that port 25 is typically reserved in hlq.PROFILE.TCPIP for the SMTP server to accept incoming mail. If another port number is selected for the SMTP server, then update the hlq.PROFILE.TCPIP file accordingly.



TCP/IP - Port Configuration Statement Syntax

```
>>-PORT----+-num--+-TCP-+--+-RESERVED---------------+-------------------+-+-><
           |      '-UDP-'  '-jobname--+-------------+-'                   |
           |                          '-| Options |-'                     |
           |                                               .-WHENLISTEN-. |
           '-UNRSV--+-TCP--+-jobname--+-------------+-+--+------------+-+-'
                    |      |          '-SAF resname-' |  '-WHENBIND---' |
                    |      '-*--+-------------+-------'                 |
                    |           +-DENY--------+                         |
                    |           '-SAF resname-'                         |
                    |                                  .-WHENBIND-.     |
                    '-UDP--+-jobname--+-------------+-+--+----------+---'
                           |          '-SAF resname-' |
                           '-*--+-------------+-------'
                                +-DENY--------+
                                '-SAF resname-'
```

Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012 - Volume 4

Note – TCP/IP Profile DECK, IPSECURITY Keyword on the IPCONFIG Statement

Legacy Security?

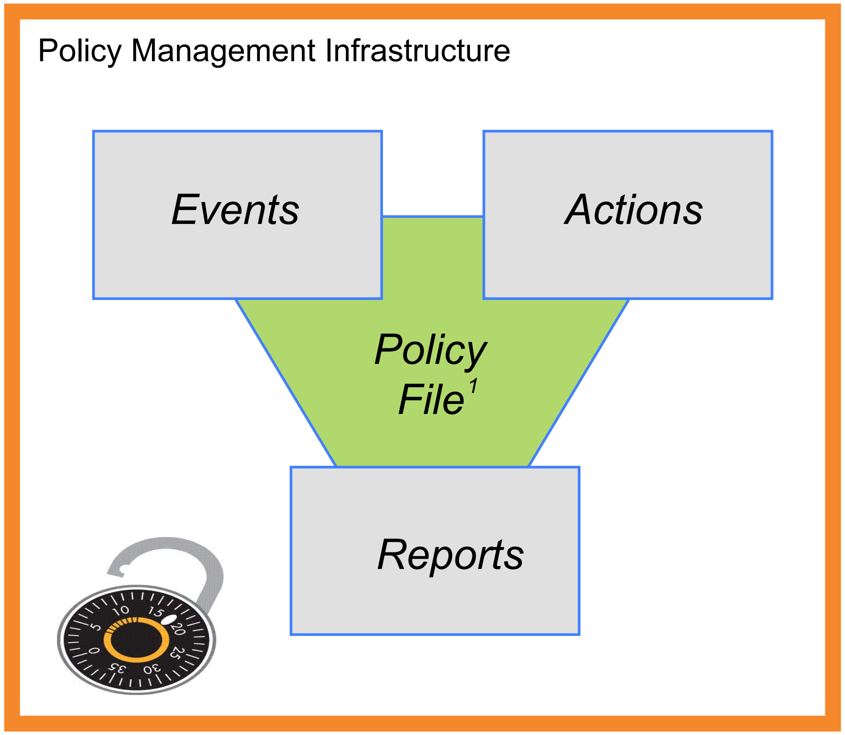
We're all under Attack! > Exploit Policy Management > It's Free

☑ Management Policies are a pre-defined set of network Events, corresponding reply Actions, related Notifications and Reports.

☑ Policy files are created and maintained using the z/OSMF Configuration Assistant, or the PC-based Configuration Assistant for the z/OS Communication Server. (Gone in V2R1)

☑ The same Policy Configuration can be applied across multiple IP Stacks in the same underlying LPAR and or LPARs.

☑ Alternatively a Unique Policy Configuration can be deployed to each IP Stack in an LPAR.



[1] /etc/cfgasst/v1r13/imagename/stackname/idsPol

Source: V1R13 IBM Configuration Assistant for z/OS Communications Server tool

Note - In V2R1, z/OSMF Takes over these configuration functions.

Legacy Security?

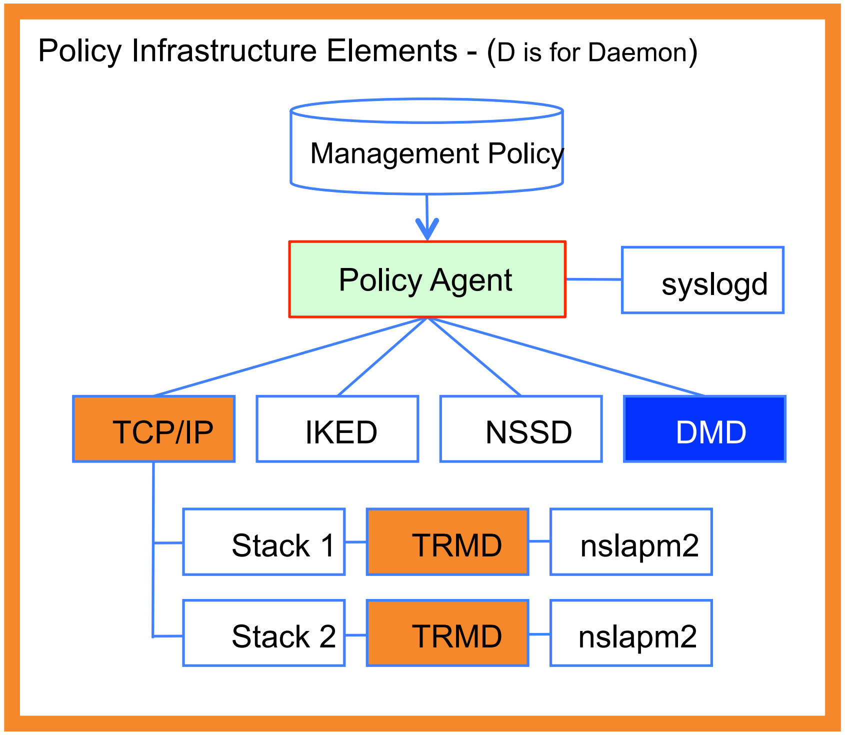
We're all under Attack! > Exploit Policy Management > It's Free

☑ PAGENT, a z/OS address space, builds the Policy Infrastructure needed by the z/OS Communication Server to support Intrusion Detection Services (IDS). PAGENT acts as a:

- ✓ Policy Server: executes on a single system and installs policies for others
- ✓ Policy Client: retrieves remote policies from the Policy Server.

☑ The Policy Infrastructure Includes:

- ✓ Internet Key Exchange (IKED)
- ✓ Network Security Services (NSSD)
- → ✓ Defense Manager (DMD)
- → ✓ Traffic Regulation Management (TRMD)
- ✓ The Reporting Subagent (nslapm2)


Policy Infrastructure Elements - (D is for Daemon)

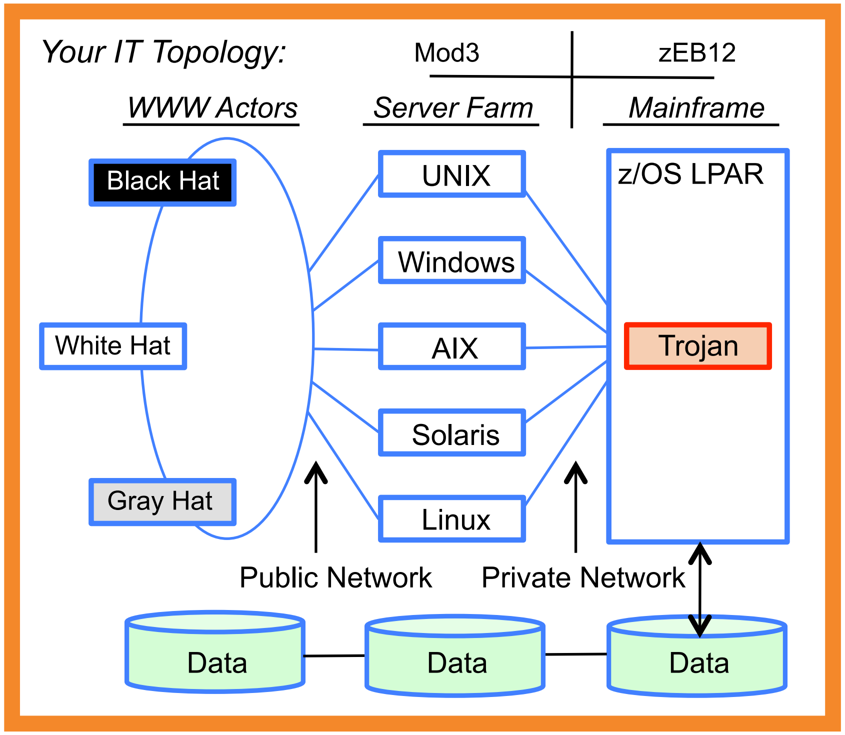
Source: V1R13 IBM Configuration Assistant for z/OS Communications Server tool
Note - In V2R1, z/OSMF Takes over these configuration functions.

Legacy Security?

We're all under Attack! > Internal Threat > The Nefarious Insider

☑ An attack against a z/OS Mainframe that is networked to a heterogeneous Server Farm could unfold as follows:

1. Scan the Server Farm for open ports
2. Send a malformed Packet to all
3. Open the packet and activate a port
4. Send a Trojan to the open server(s)
5. Begin scan for open mainframe port
6. Send malformed Packet to one
7. Open the packet and Logon
8. Begin scanning for Relevant Data
9. FTP Data to Internet Drop Box
10. Terminate and Erase Self



Source: All that have been cited up to this point!
Note - Denial-of-Service (DoS) Attacks, Man-in-the-middle attacks

Legacy Security?

We're all under Attack! > Internal Threat > Configuration Controls

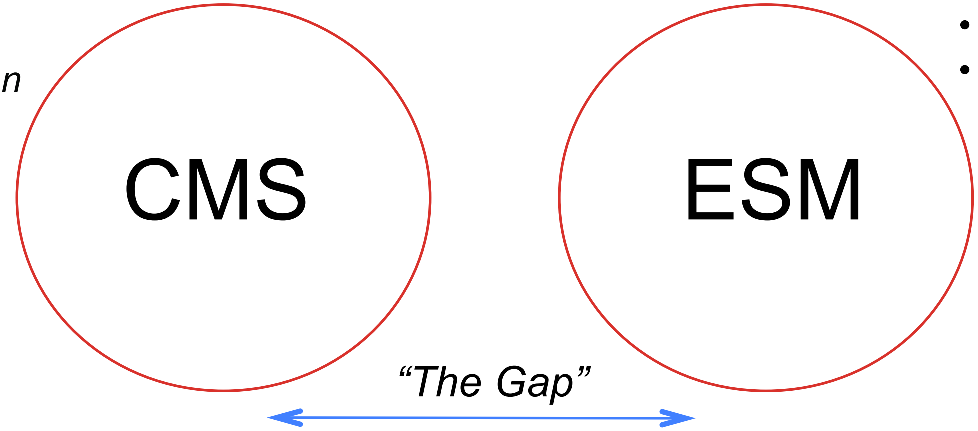
zEnterprise System Integrity - Exposing "The Gap" between CMS and ESM.

CMS: Change Management System

- *Planning*
- *Authorization*

ESM: External Security Manager

- *Access Rights*
- *Update Privileges*


CMS

ESM

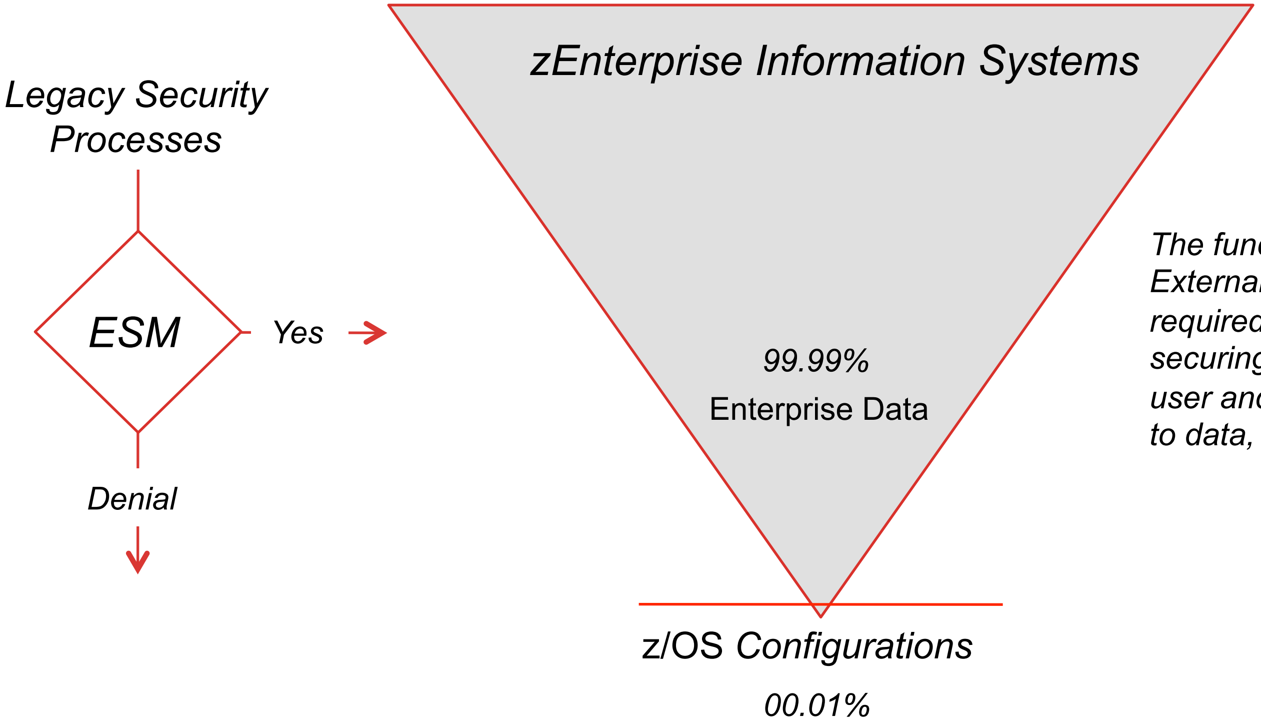
"The Gap"

Lack of Documentation
and "Refined" Access Control
at the
Point of the Actual Change

Legacy Security?

We're all under Attack! > Internal Threat > Configuration Controls

zEnterprise System Integrity - All Rest on z/OS Configuration Definitions



Legacy Security Processes

ESM

Yes

Denial

zEnterprise Information Systems

99.99%

Enterprise Data

z/OS Configurations

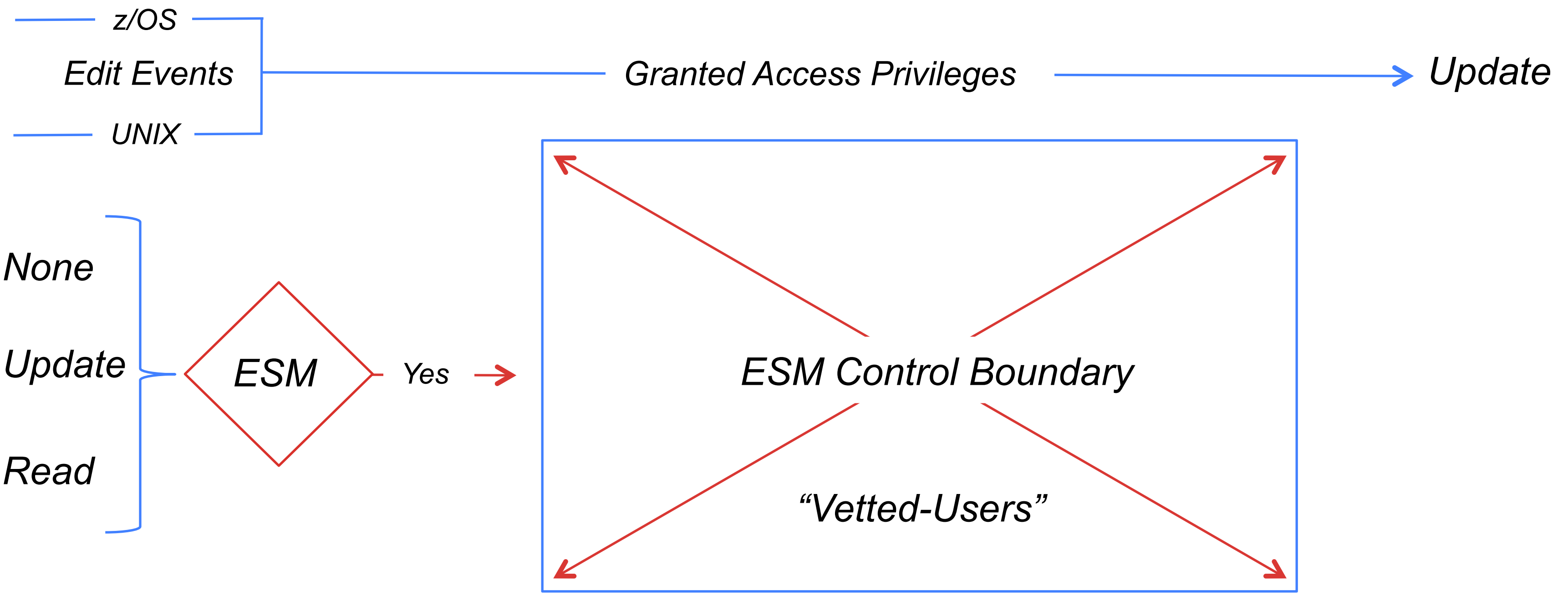
00.01%

The functions provided by the External Security Manager (ESM) are required, absolute and unmatched for securing, granting and/or denying user and/or processes access system to data, resources and commands.

Legacy Security?

We're all under Attack! > Internal Threat > Configuration Controls

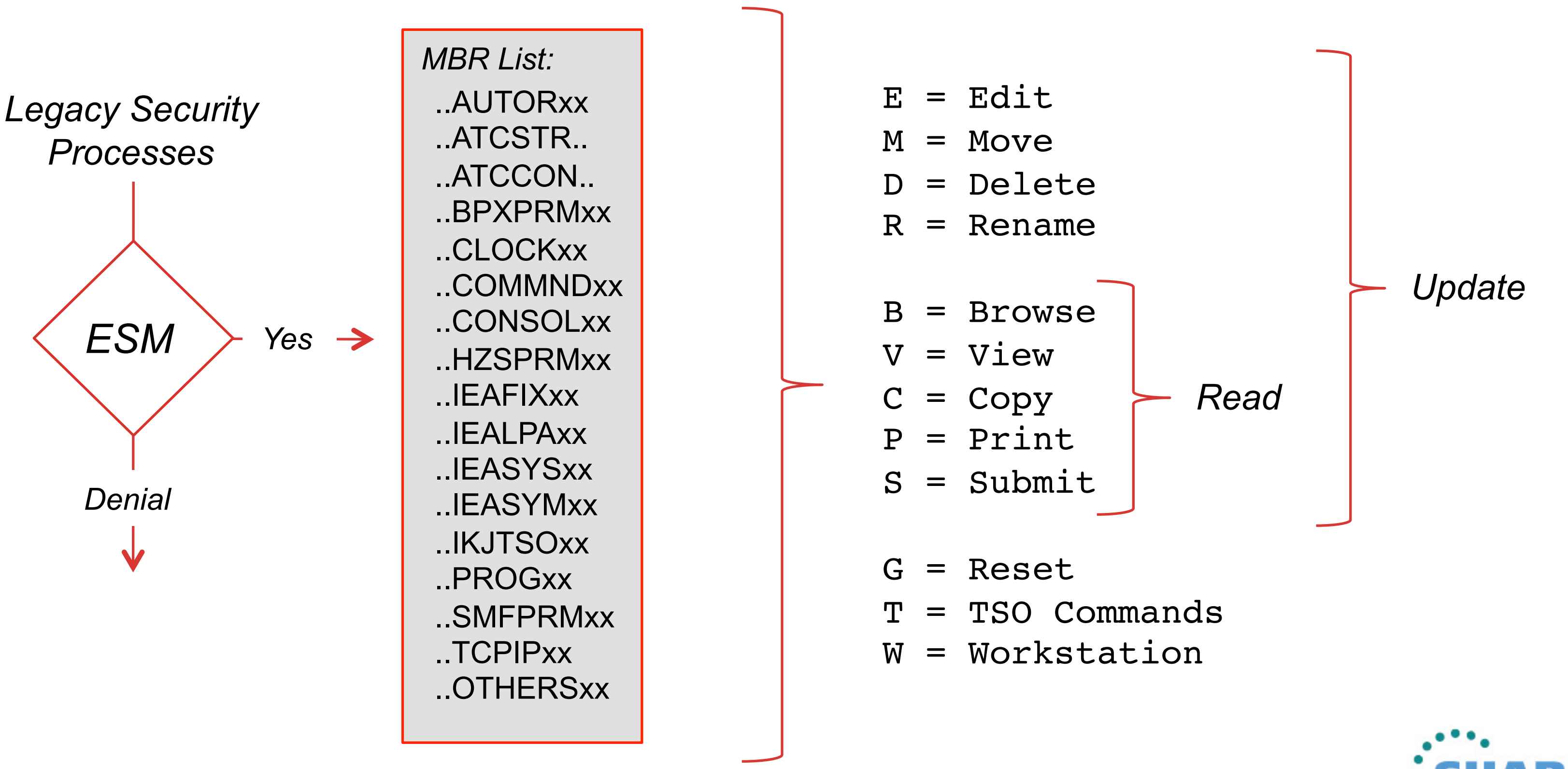
zEnterprise System Integrity - Dataset access allowed to "Vetted-Users"



Legacy Security?

We're all under Attack! > Internal Threat > Configuration Controls

zEnterprise System Integrity - Member List and Member Selection Options



Legacy Security Processes

ESM

Yes

Denial

MBR List:

..AUTORxx
..ATCSTR..
..ATCCON..
..BPXPRMxx
..CLOCKxx
..COMMNDxx
..CONSOLxx
..HZSPRMxx
..IEAFIXxx
..IEALPAxx
..IEASYSxx
..IEASYMxx
..IKJTSOxx
..PROGxx
..SMFPRMxx
..TCPIPxx
..OTHERSxx

```
E = Edit
M = Move
D = Delete
R = Rename

B = Browse
V = View
C = Copy
P = Print
S = Submit

G = Reset
T = TSO Commands
W = Workstation
```

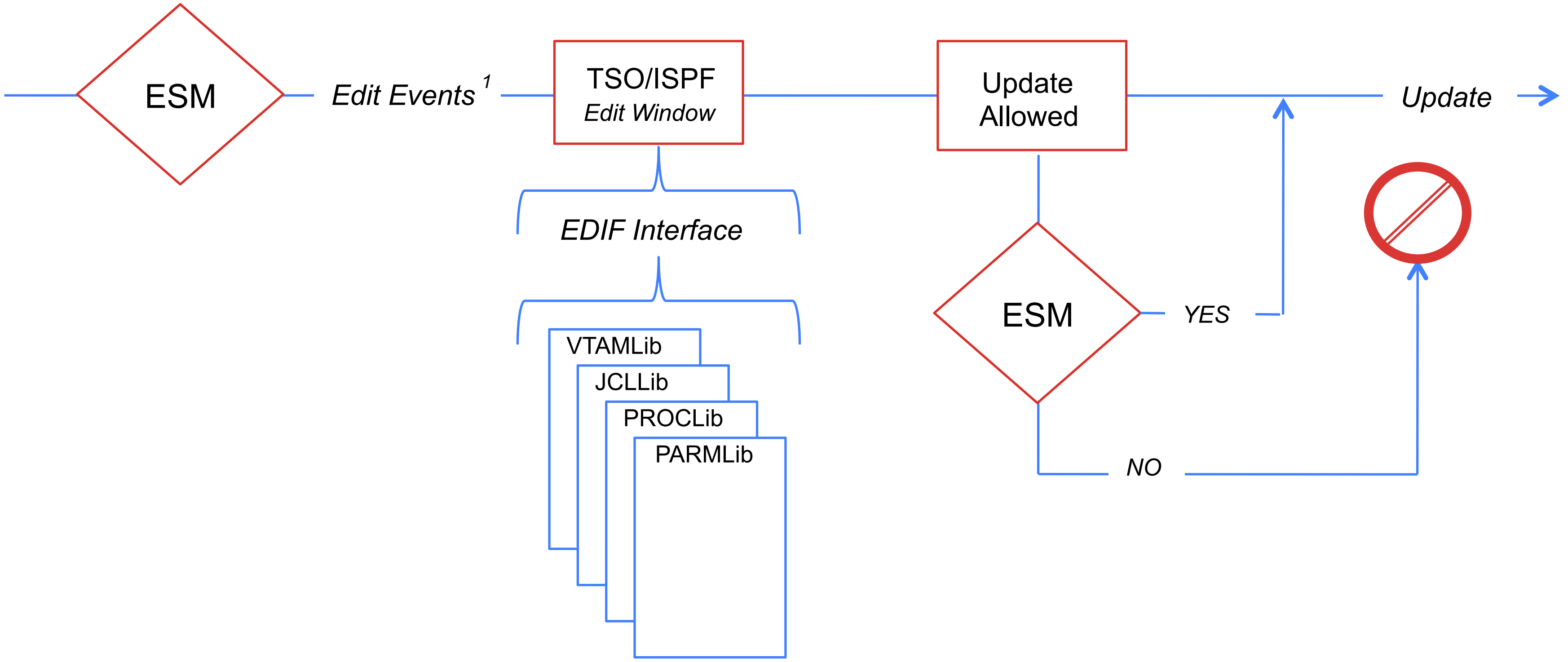
Read

Update

Legacy Security?

We're all under Attack! > Internal Threat > Closing "The Gap"

zEnterprise System Integrity - Model of an interactive z/OS Update.



[1] z/OS, z/UNIX

Legacy Security?

We're all under Attack! > Internal Threat > Closing "The Gap"

zEnterprise System Integrity - EDIF Services - What do they Provide?

The Edit Interface (EDIF)[1]service provides edit functions for data accessed through dialog-supplied I/O routines. The dialog intercept must perform all environment-dependent functions such as dataset allocation, opening, reading, writing, closing, and freeing.

The dialog is also responsible for any necessary ENQ/DEQ serialization.

On Entry - Application Control:

- pre-processing that can allow/deny dataset/member access, detect changes, create backups,
- editing data in partitioned datasets and sequential files and
- post-processing can detect changes, displays inline descriptor information, generates optional occurrence notification and refreshes a backup as needed.

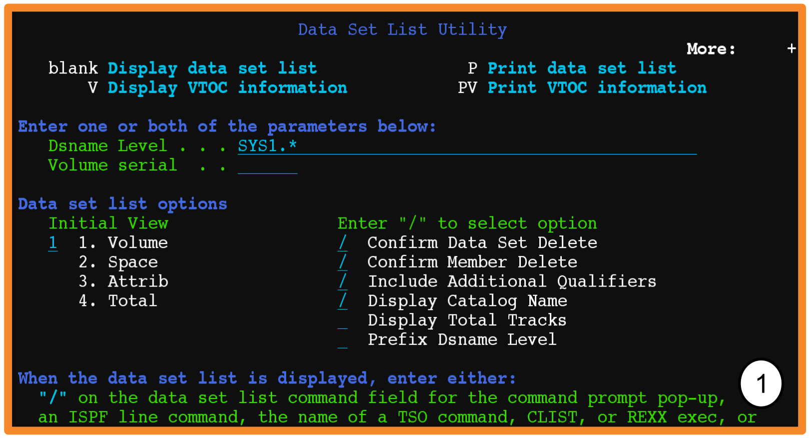
On Exit - Application Control:

- provides routines that perform data read and write operations,
- provides command processing to support MOVE, COPY, CREATE, REPLACE, and the EDIT primary commands and
- supports unique application specific TSO/ISPF primary line commands.

[1] *For more on EDIF and the "Edit Window" see the z/OS V1R13.0 ISPF Services Guide*

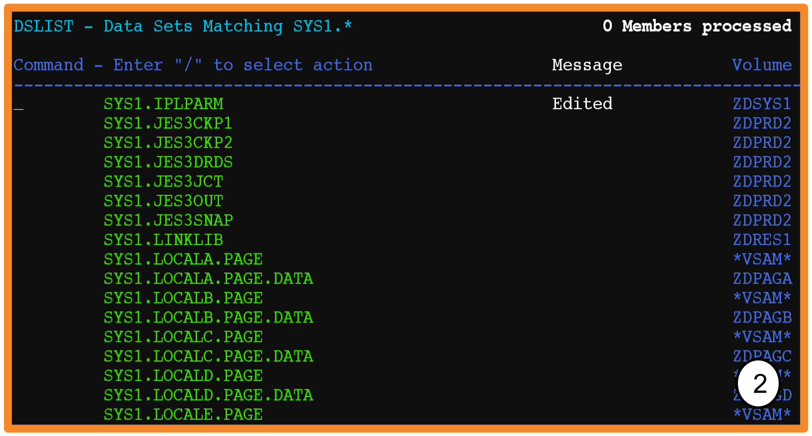
Legacy Security?

We're all under Attack! > Internal Threat > Closing "The Gap"



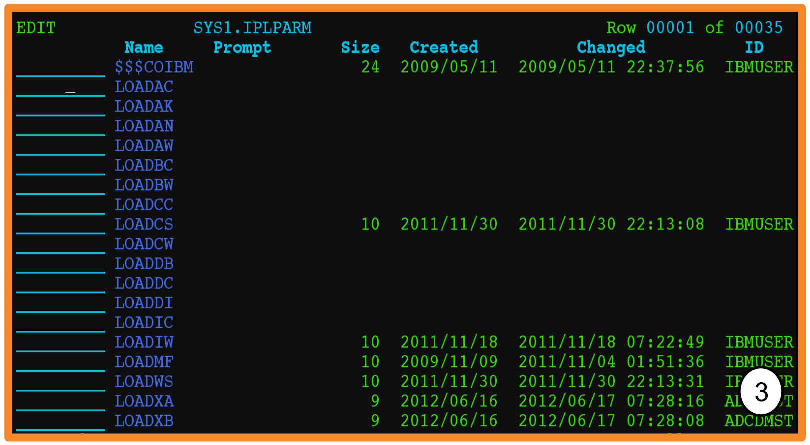
```
                       Data Set List Utility
                                                                More:     +
   blank Display data set list                  P  Print data set list
       V Display VTOC information               PV Print VTOC information

Enter one or both of the parameters below:
   Dsname Level . . . SYS1.*
   Volume serial  . . ______

Data set list options
   Initial View                Enter "/" to select option
   1  1. Volume                /  Confirm Data Set Delete
      2. Space                 /  Confirm Member Delete
      3. Attrib                /  Include Additional Qualifiers
      4. Total                 /  Display Catalog Name
                               _  Display Total Tracks
                               _  Prefix Dsname Level

When the data set list is displayed, enter either:
  "/" on the data set list command field for the command prompt pop-up,
  an ISPF line command, the name of a TSO command, CLIST, or REXX exec, or
```

1



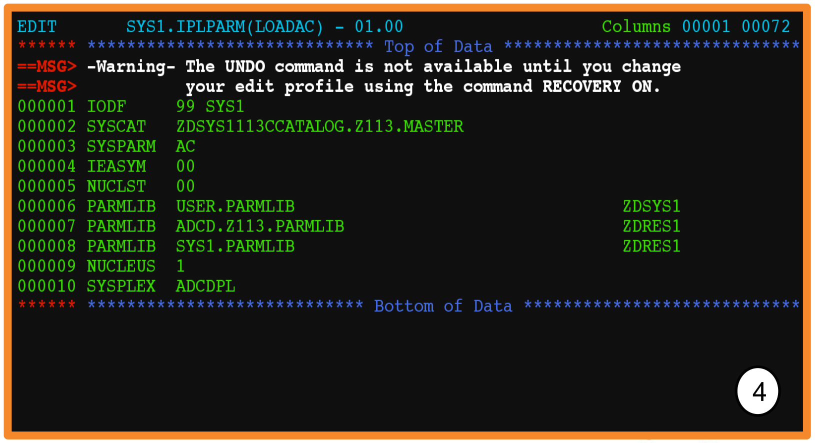
```
DSLIST - Data Sets Matching SYS1.*                            0 Members processed

Command - Enter "/" to select action                      Message          Volume
-----------------------------------------------------------------------------------
_        SYS1.IPLPARM                                     Edited           ZDSYS1
         SYS1.JES3CKP1                                                     ZDPRD2
         SYS1.JES3CKP2                                                     ZDPRD2
         SYS1.JES3DRDS                                                     ZDPRD2
         SYS1.JES3JCT                                                      ZDPRD2
         SYS1.JES3OUT                                                      ZDPRD2
         SYS1.JES3SNAP                                                     ZDPRD2
         SYS1.LINKLIB                                                      ZDRES1
         SYS1.LOCALA.PAGE                                                  *VSAM*
         SYS1.LOCALA.PAGE.DATA                                             ZDPAGA
         SYS1.LOCALB.PAGE                                                  *VSAM*
         SYS1.LOCALB.PAGE.DATA                                             ZDPAGB
         SYS1.LOCALC.PAGE                                                  *VSAM*
         SYS1.LOCALC.PAGE.DATA                                             ZDPAGC
         SYS1.LOCALD.PAGE                                                  *VSAM*
         SYS1.LOCALD.PAGE.DATA                                             ZDPAGD
         SYS1.LOCALE.PAGE                                                  *VSAM*
```

2



```
EDIT             SYS1.IPLPARM                               Row 00001 of 00035
           Name     Prompt         Size   Created           Changed          ID
_________ $$$COIBM                   24  2009/05/11  2009/05/11 22:37:56  IBMUSER
______ _  LOADAC
_________ LOADAK
_________ LOADAN
_________ LOADAW
_________ LOADBC
_________ LOADBW
_________ LOADCC
_________ LOADCS                     10  2011/11/30  2011/11/30 22:13:08  IBMUSER
_________ LOADCW
_________ LOADDB
_________ LOADDC
_________ LOADDI
_________ LOADIC
_________ LOADIW                     10  2011/11/18  2011/11/18 07:22:49  IBMUSER
_________ LOADMF                     10  2009/11/09  2011/11/04 01:51:36  IBMUSER
_________ LOADWS                     10  2011/11/30  2011/11/30 22:13:31  IBMUSER
_________ LOADXA                      9  2012/06/16  2012/06/17 07:28:16  ADCDMST
_________ LOADXB                      9  2012/06/16  2012/06/17 07:28:08  ADCDMST
```

3

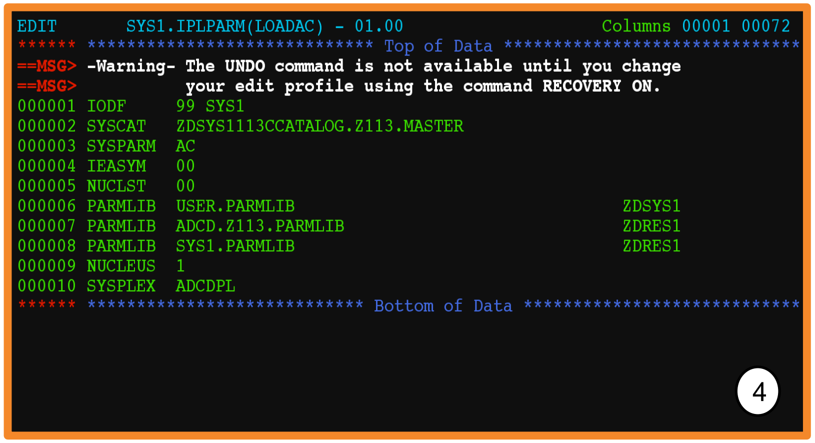


```
EDIT       SYS1.IPLPARM(LOADAC) - 01.00                     Columns 00001 00072
****** **************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 IODF     99 SYS1
000002 SYSCAT   ZDSYS1113CCATALOG.Z113.MASTER
000003 SYSPARM  AC
000004 IEASYM   00
000005 NUCLST   00
000006 PARMLIB  USER.PARMLIB                                ZDSYS1
000007 PARMLIB  ADCD.Z113.PARMLIB                           ZDRES1
000008 PARMLIB  SYS1.PARMLIB                                ZDRES1
000009 NUCLEUS  1
000010 SYSPLEX  ADCDPL
****** **************************** Bottom of Data ****************************
```

4

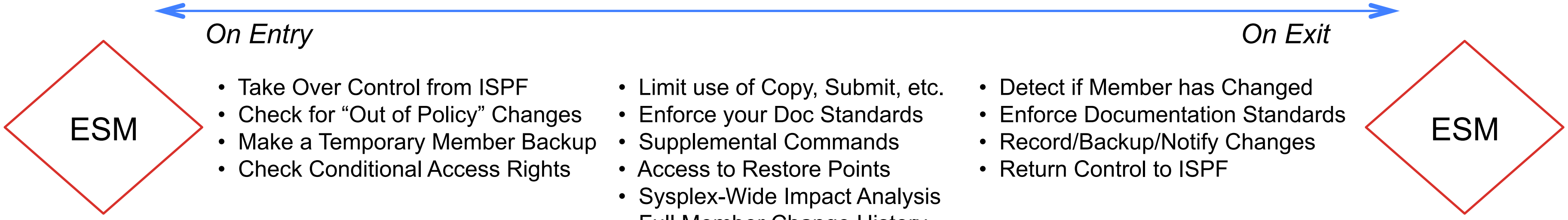
Legacy Security?

We're all under Attack! > Internal Threat > Closing "The Gap"



```
EDIT       SYS1.IPLPARM(LOADAC) - 01.00                    Columns 00001 00072
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 IODF     99 SYS1
000002 SYSCAT   ZDSYS1113CCATALOG.Z113.MASTER
000003 SYSPARM  AC
000004 IEASYM   00
000005 NUCLST   00
000006 PARMLIB  USER.PARMLIB                                 ZDSYS1
000007 PARMLIB  ADCD.Z113.PARMLIB                            ZDRES1
000008 PARMLIB  SYS1.PARMLIB                                 ZDRES1
000009 NUCLEUS  1
000010 SYSPLEX  ADCDPL
****** **************************** Bottom of Data ****************************
```

Custom Application Shares Control with ISPF



On Entry

- Take Over Control from ISPF
- Check for "Out of Policy" Changes
- Make a Temporary Member Backup
- Check Conditional Access Rights

- Limit use of Copy, Submit, etc.
- Enforce your Doc Standards
- Supplemental Commands
- Access to Restore Points
- Sysplex-Wide Impact Analysis
- Full Member Change History
- Change Testing and Validation

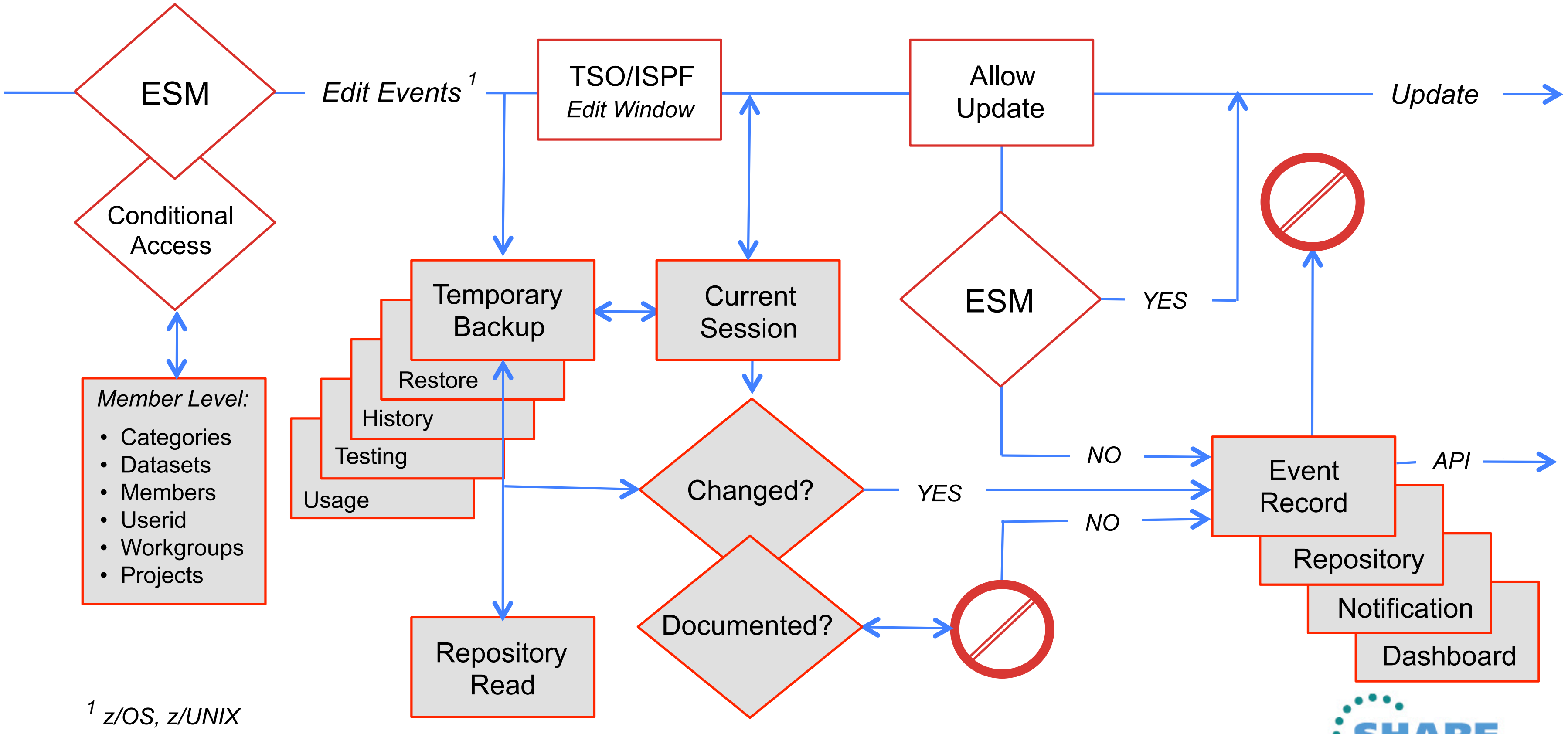
On Exit

- Detect if Member has Changed
- Enforce Documentation Standards
- Record/Backup/Notify Changes
- Return Control to ISPF

Legacy Security?

We're all under Attack! > Internal Threat > Closing "The Gap"

zEnterprise System Integrity - EDIF Services - Improving Work Flow?

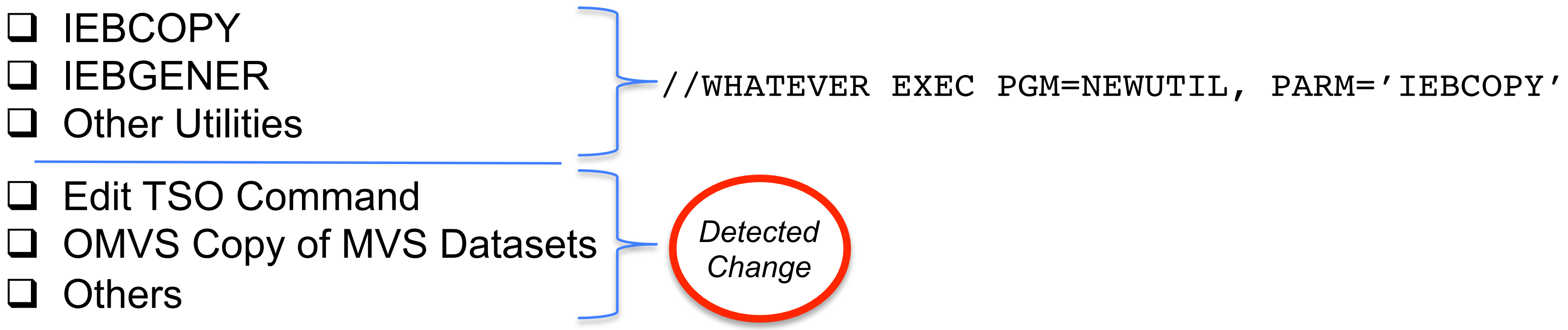


[1] z/OS, z/UNIX

Legacy Security?

We're all under Attack! > Internal Threat > Closing "The Gap"

zEnterprise System Integrity - Batch Utilities and Detected Changes



□ IEBCOPY
□ IEBGENER
□ Other Utilities

```
//WHATEVER EXEC PGM=NEWUTIL, PARM='IEBCOPY'
```

□ Edit TSO Command
□ OMVS Copy of MVS Datasets
□ Others

Detected Change

Detected Change: Must be an automated programmatic process by which the actual content of datasets defined to TCE as "Controlled Datasets" is reconciled with the last TCE Control Journal Copy. This reconciliation is performed at a minimum hourly and in all cases before the results of any query, report or panel is made available.

Legacy Security?

We’re all under Attack! > Internal Threat > Closing “The Gap”

zEnterprise System Integrity - Collecting Change Documentation

de·scrip·tor [1]

A noun

/diˈskriptər/

1. An element or term that has the function of describing, identifying, or indexing, in particular.
2. A word or expression used to describe or identify something.
3. Descriptors are also used to hold information about data that is only fully known at run-time, such as a [dynamically allocated array.]

[1] *Source: http://en.wikipedia.org/wiki/Data_descriptor*

Legacy Security?

We're all under Attack! > Regulatory Threats > Data "Copies"

☑ "Copies" now 70% of Mainframe Data.

- Developers and QA personnel made copies
- Their co-workers made copies of copies
- Query results and reports make copies

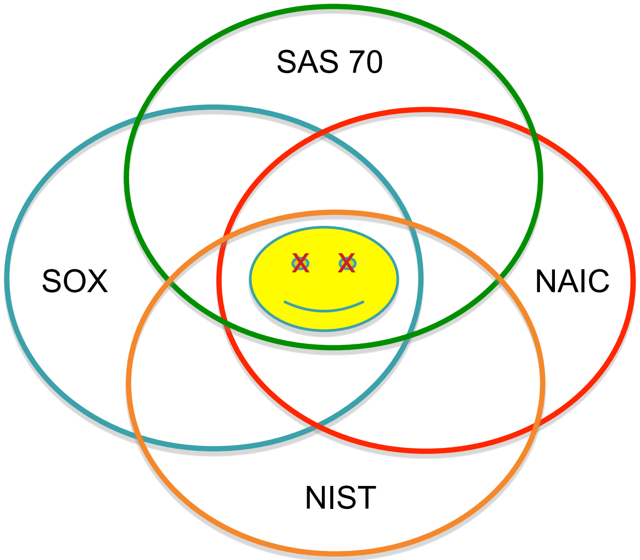
☑ "Copies" are rarely deleted!

☑ "Copies" often contain sensitive data:

- PCI, HIPAA, SOX, IP, etc.

☑ "Copies" unknown to the Data Security Team cannot possibly be "*properly*" protected using the access rule used by the External Security Manger (ESM).

You Cannot Protect what You Don't Know Exits!



Not knowing can be a very Risky Business!

Legacy Security?

We're all under Attack! > Regulatory Threats > Xbridge Systems

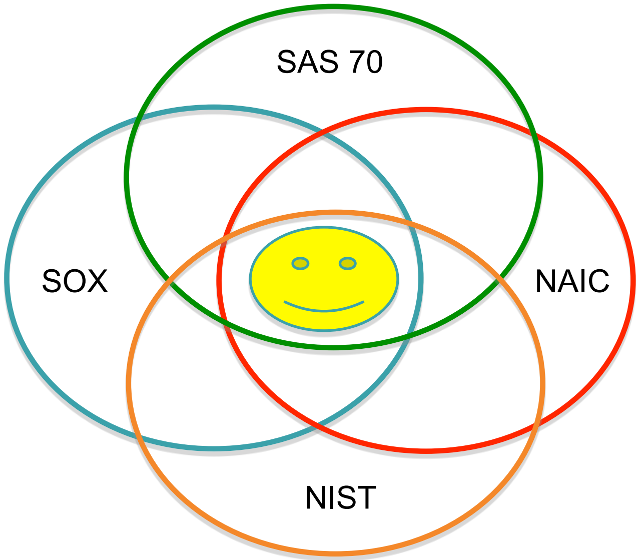
☑ The right tools can help you to eliminate most of the "Copies" and in doing so the Regulatory Threat. They Automatically:

- Locate Sensitive Dataset Copies.
- Isolate Sensitive Database Tables.
- Deal with Data Migration Issues.

☑ Best Practices can help as well:

- Datasets not recently referenced identified and stored securely.
- Database tables currently in use should have access authorities validated.
- Maintain a record of all Datasets by Type with a reference to the date of last use.

Let the DATASNIFF Open Your Eyes!



Eliminate most of the data, eliminate most of the risk!

Legacy Security?

We're all under Attack! > Regulatory Threats > Vanguard Integrity

☑ DISA, The Defense Information Systems Agency, recently issued new Security Guidelines:

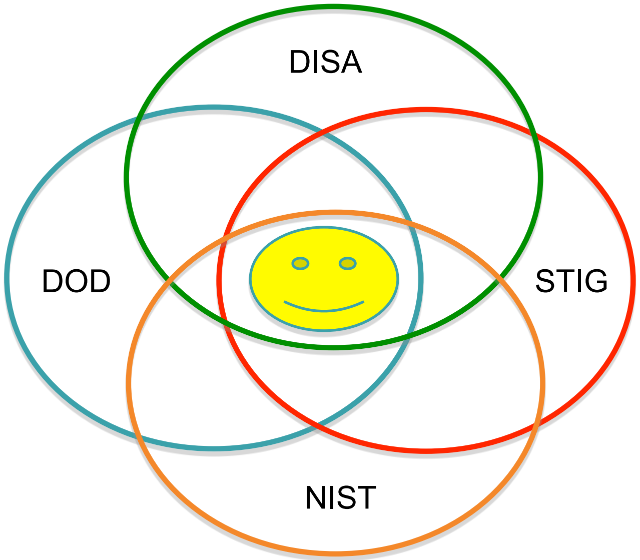
The Security Technical Implementation Guide

☑ The "STIG" Database contains known security configuration concerns, vulnerabilities, and issues required to be addressed by DOD policy.

☑ DOD requirements that "information assurance (IA) and IA-enabled IT products incorporated into DOD IS shall be configured in accordance with STIG configuration guidelines".

☑ Implementing the recommendations in STIG will ensure that DOD environments meet desired security requirements.

You Cannot Protect what You Don't Know Exits!



Not knowing can be a very Risky Business!

Legacy Security?

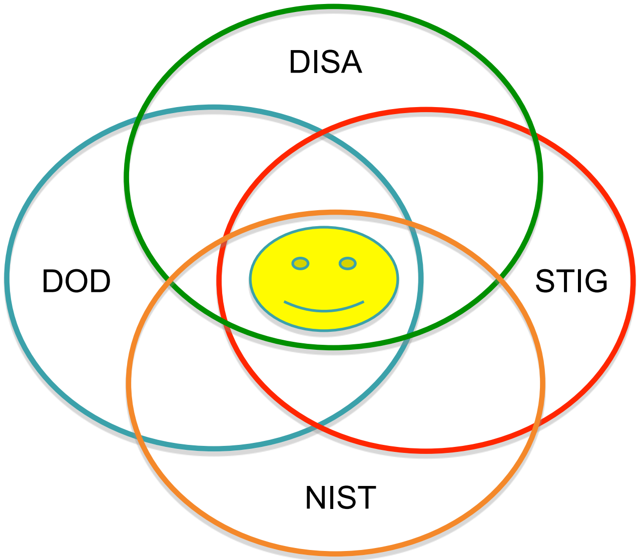
We're all under Attack! > Regulatory Threats > Vanguard Integrity

☑ Automatically detect and notify personnel when threat events on the mainframe and network occur, then respond to deviations from the security baseline with corrective actions that reassert the approved security policy.

☑ Satisfy the demands of Regulatory Compliance Standards (i.e. STIG) that require continuous oversight to ensure that approved IS controls (i.e. DOD) are in place and will stay that way.

☑ Gain confidence that their z/OS and RACF security implementations are protecting critical data and resources and are continuously in adherence to z/OS best practices.

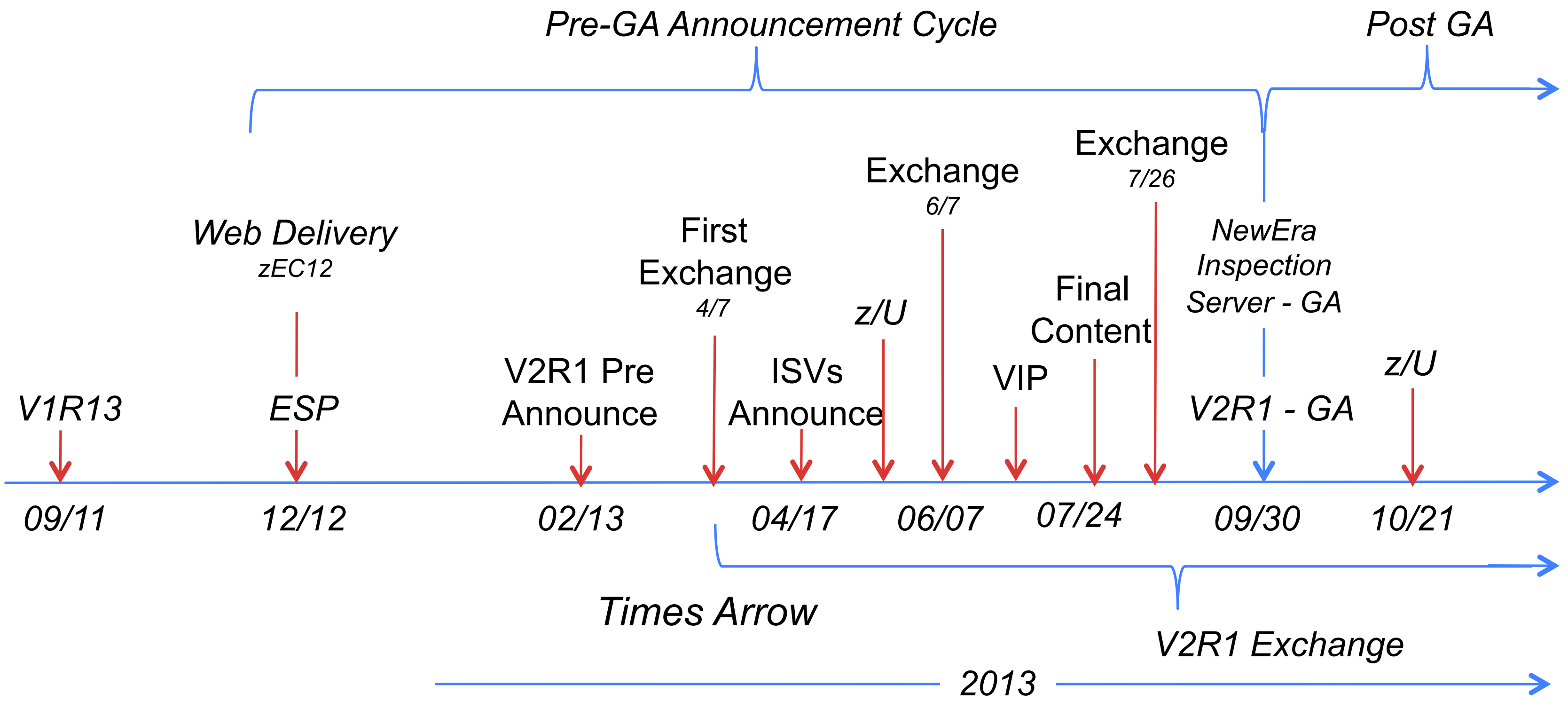
Enforcer - Common Criteria (EAL 3+) Certified!



Adherence to "Standards" eliminates most of the risk!

Legacy Security?

The Future of Security > V2R1 > Timeline > GA 09/30/2013



Pre-GA Announcement Cycle

Post GA

Web Delivery
zEC12

First Exchange
4/7

Exchange
6/7

Exchange
7/26

NewEra Inspection Server - GA

z/U

Final Content

V1R13

ESP

V2R1 Pre Announce

ISVs Announce

VIP

V2R1 - GA

z/U

09/11 *12/12* *02/13* *04/17* *06/07* *07/24* *09/30* *10/21*

Times Arrow

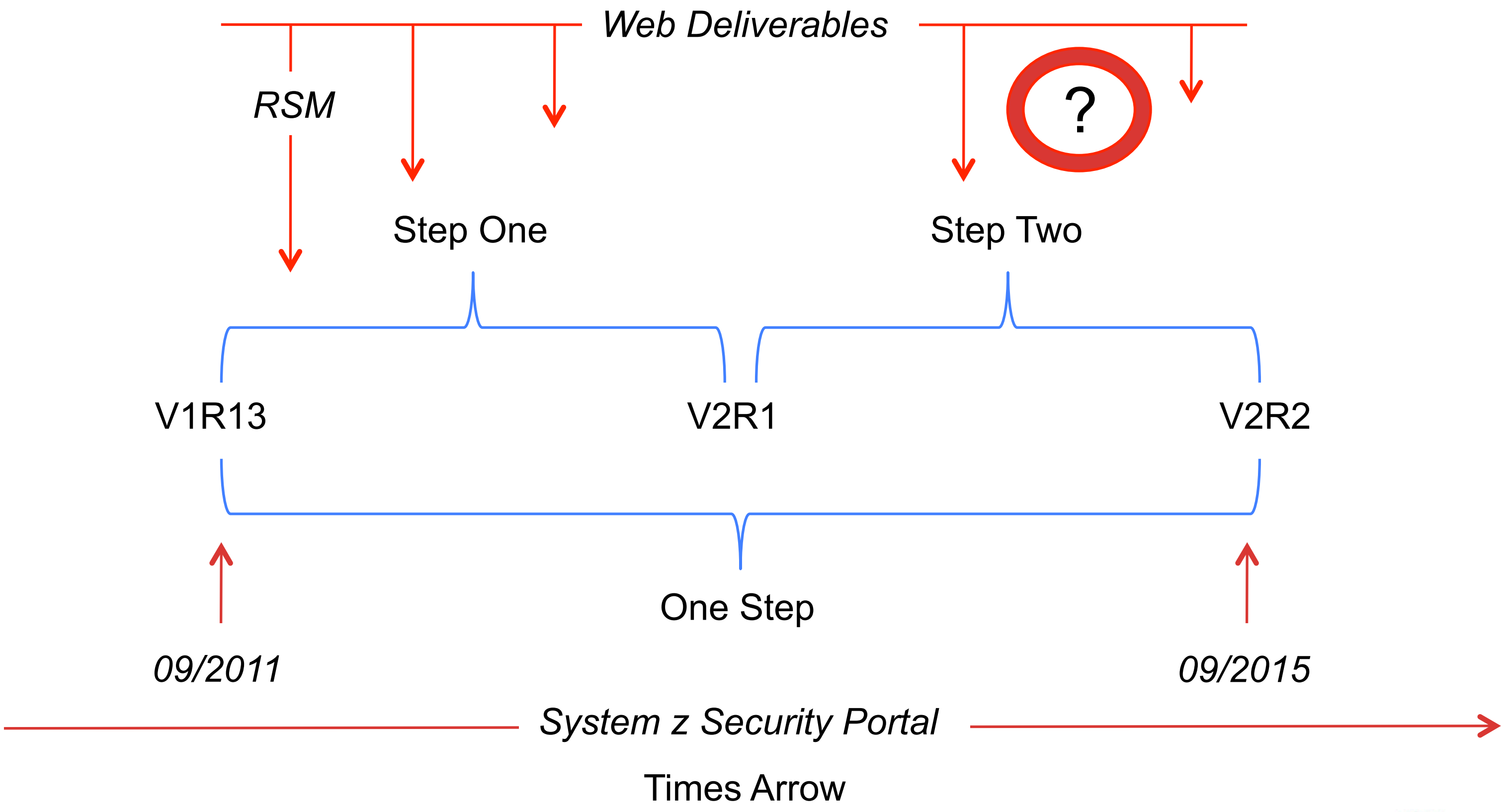
V2R1 Exchange

2013

Just Google V2R1 Exchange

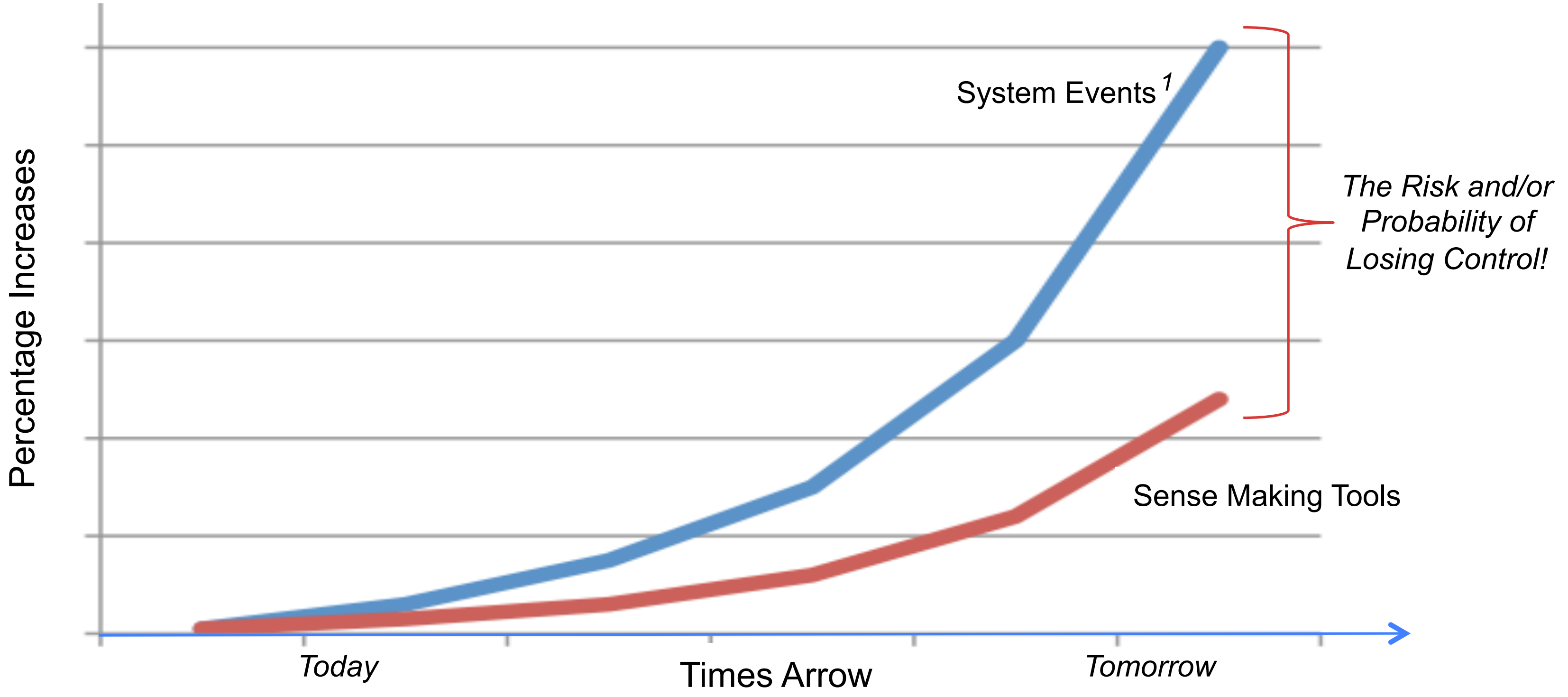
Legacy Security?

The Future of Security > V2R1 > Web Delivery > Security Portal



Legacy Security?

The Future of Security > Hyper-Performing Systems



[1] *More than 40,000 unique message IDs are defined for z/OS and the IBM software that runs on z/OS systems. In a College Dictionary (Abridged) there are 50,000 - 70,000 words*

Legacy Security?

The Future of Security > The zEnterprise, Dynamic, Global!

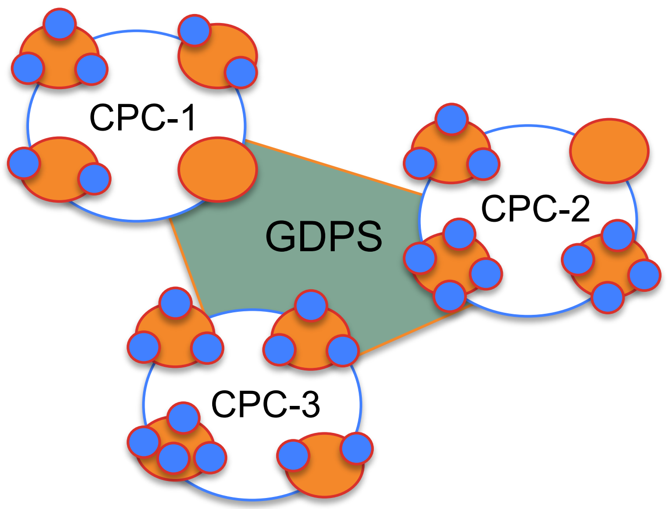
☑ *Planned Extinction via Evolution:*

Today	*Tomorrow*
• Fixed service profile →	Dynamic services
• Structured data at rest	Unstructured motion
• Personal Computers	Devices of any kind
• Stable Workloads	Unpredictable
• Static infrastructure	Cloud services
• Proprietary standards	Open innovation

☑ *Evolved Delivery will be:*

- Without Boundaries
- Fully Instrumented
- Interconnected
- Highly Intelligent

GDPS: Geographically Disbursed Sysplex

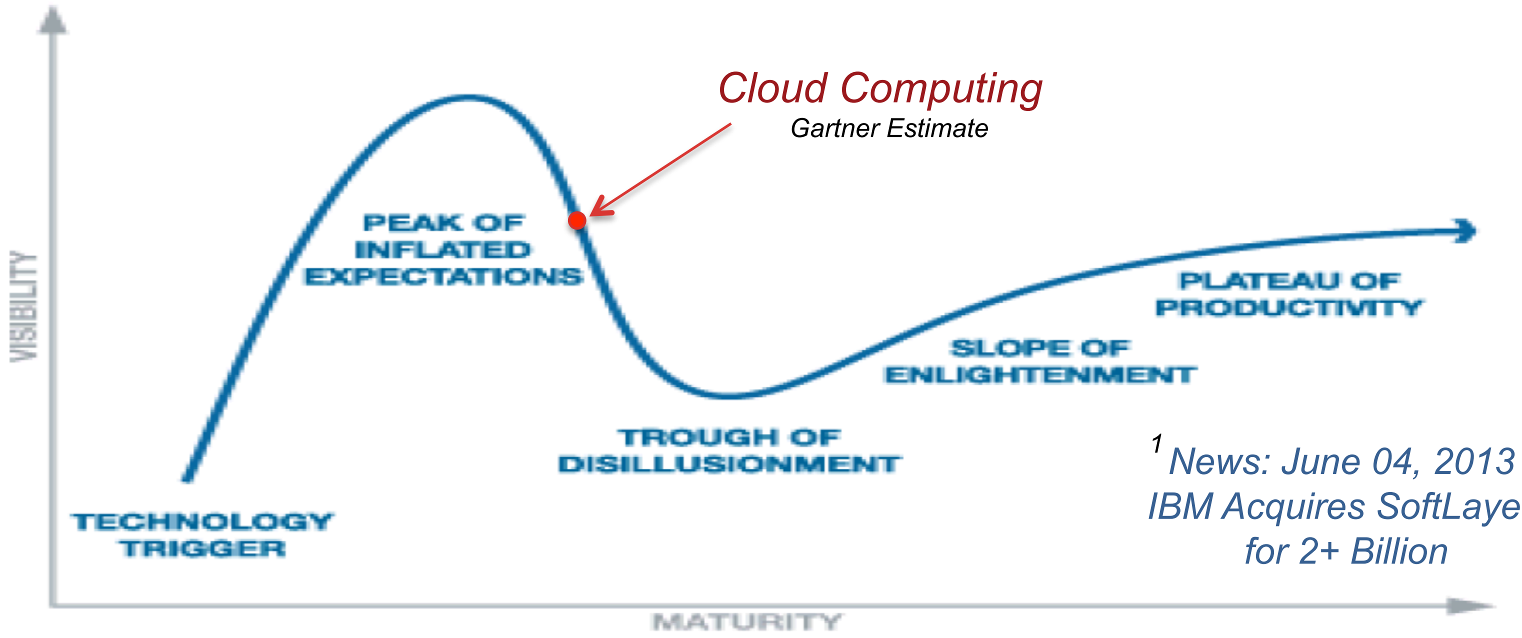


CPC: Central Processing Complex

Legacy Security?

The Future of Security > The zEnterprise, Public Vs. Private Cloud!

Does the Cloud Really Matter?

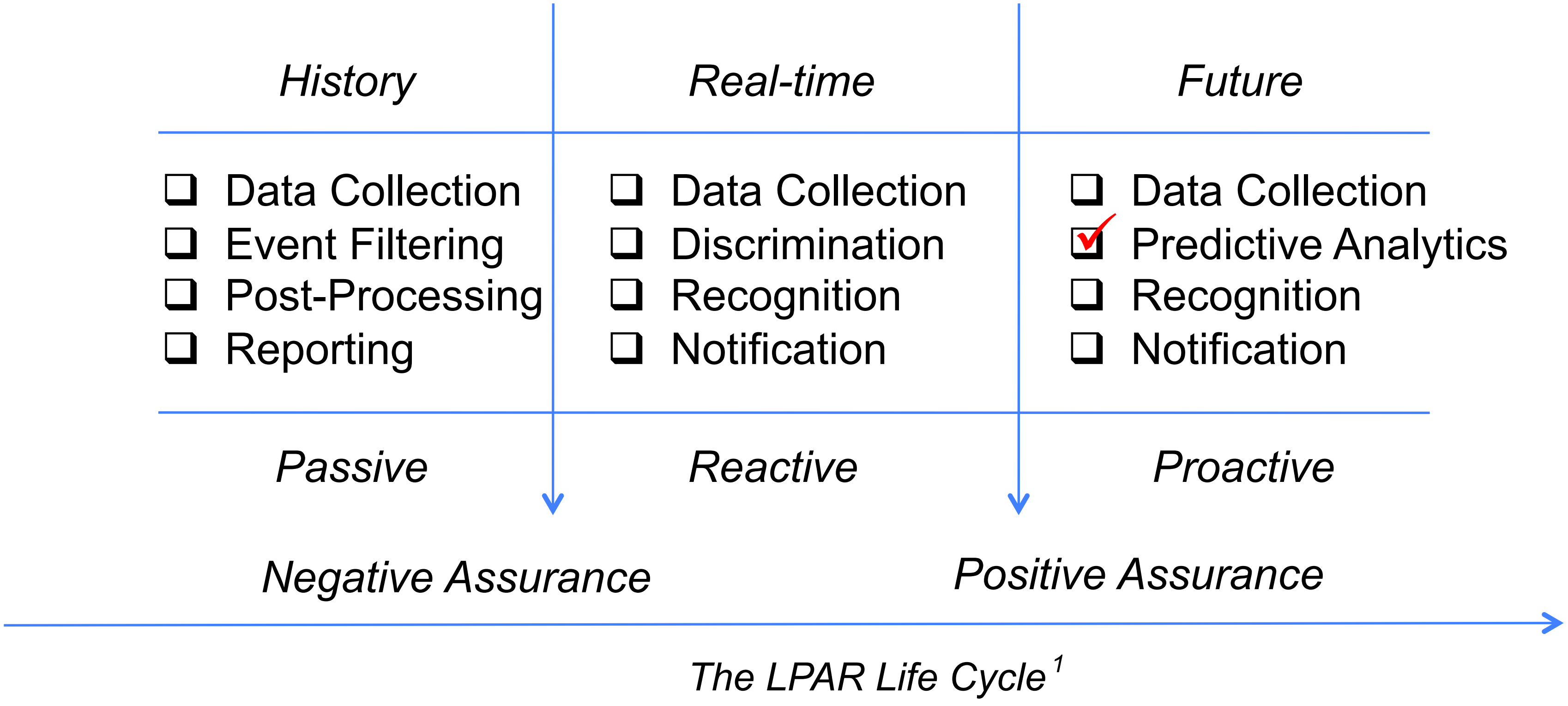


[1] News: June 04, 2013
IBM Acquires SoftLayer
for 2+ Billion

[1] *Source:http://www.forbes.com/sites/forrester/2013/06/06/ibm-buys-softlayer-but-will-they-learn-from-them/*
http://dealbook.nytimes.com/2013/06/04/i-b-m-buys-cloud-computing-firm-in-deal-said-to-be-worth-2-billion/

Legacy Security?

The Future of Security > Predictive Failure Analysis



History	*Real-time*	*Future*
□ Data Collection	□ Data Collection	□ Data Collection
□ Event Filtering	□ Discrimination	☑ Predictive Analytics
□ Post-Processing	□ Recognition	□ Recognition
□ Reporting	□ Notification	□ Notification
Passive	*Reactive*	*Proactive*

Negative Assurance

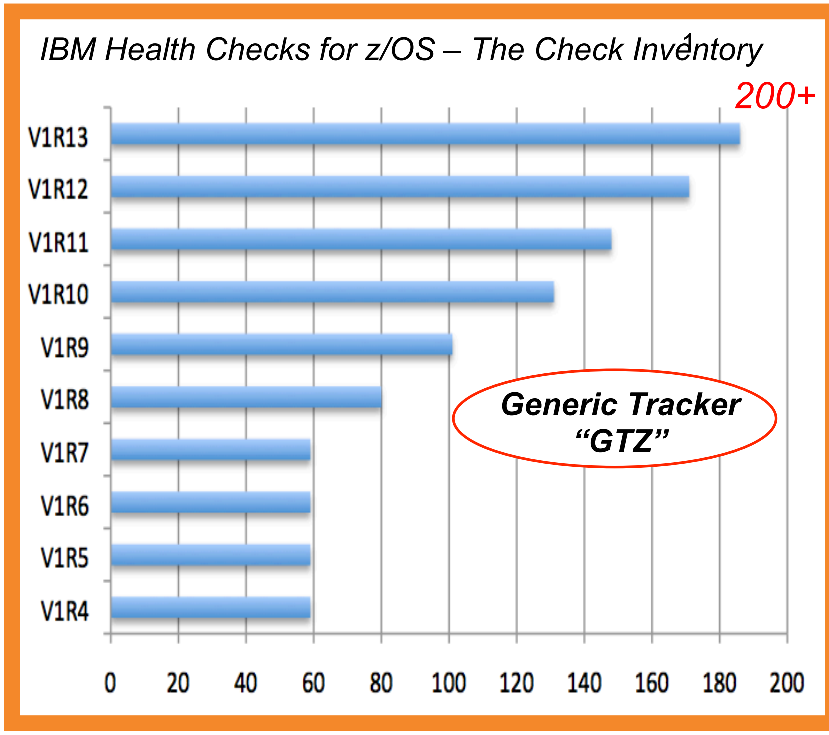
Positive Assurance

The LPAR Life Cycle[1]

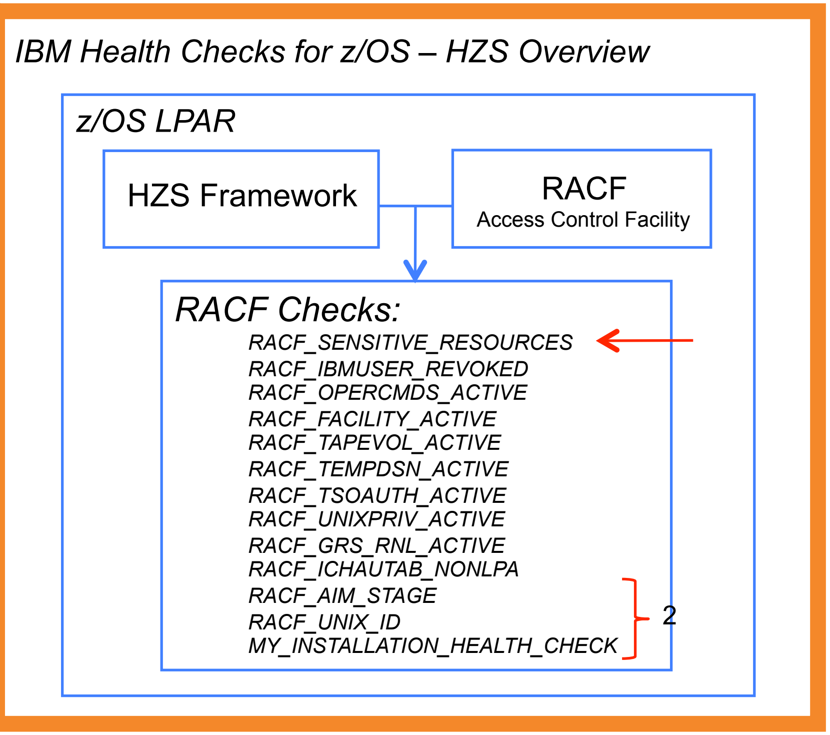
[1] *Just How Long? Day, Week, Month, Quarter, Half-Year or Full-Year*

Legacy Security?

The Future of Security > Health Checker > A Security Necessity



IBM Health Checks for z/OS – The Check Inventory[1]



IBM Health Checks for z/OS – HZS Overview

z/OS LPAR

HZS Framework

RACF
Access Control Facility

RACF Checks:

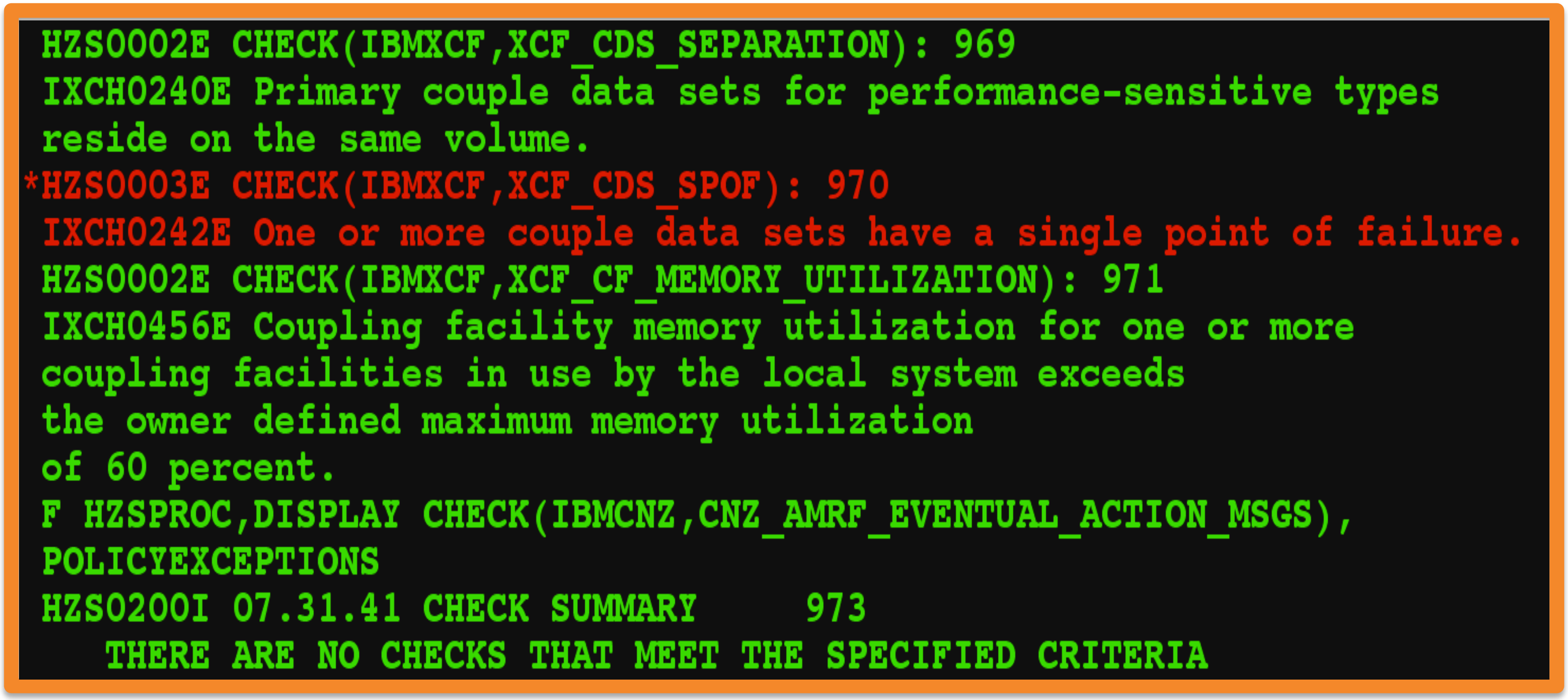
RACF_SENSITIVE_RESOURCES
RACF_IBMUSER_REVOKED
RACF_OPERCMDS_ACTIVE
RACF_FACILITY_ACTIVE
RACF_TAPEVOL_ACTIVE
RACF_TEMPDSN_ACTIVE
RACF_TSOAUTH_ACTIVE
RACF_UNIXPRIV_ACTIVE
RACF_GRS_RNL_ACTIVE
RACF_ICHAUTAB_NONLPA
RACF_AIM_STAGE
RACF_UNIX_ID
MY_INSTALLATION_HEALTH_CHECK

[1] *zZS18 – The Latest in IBM Health Checker for z/OS - Marna Walle, IBM Corporation*

[2] *Mark Nelson, z/OS Security Server (RACF) Design and Development - APAR OA37164*

Legacy Security?

The Future of Security > Health Checker > A Security Necessity



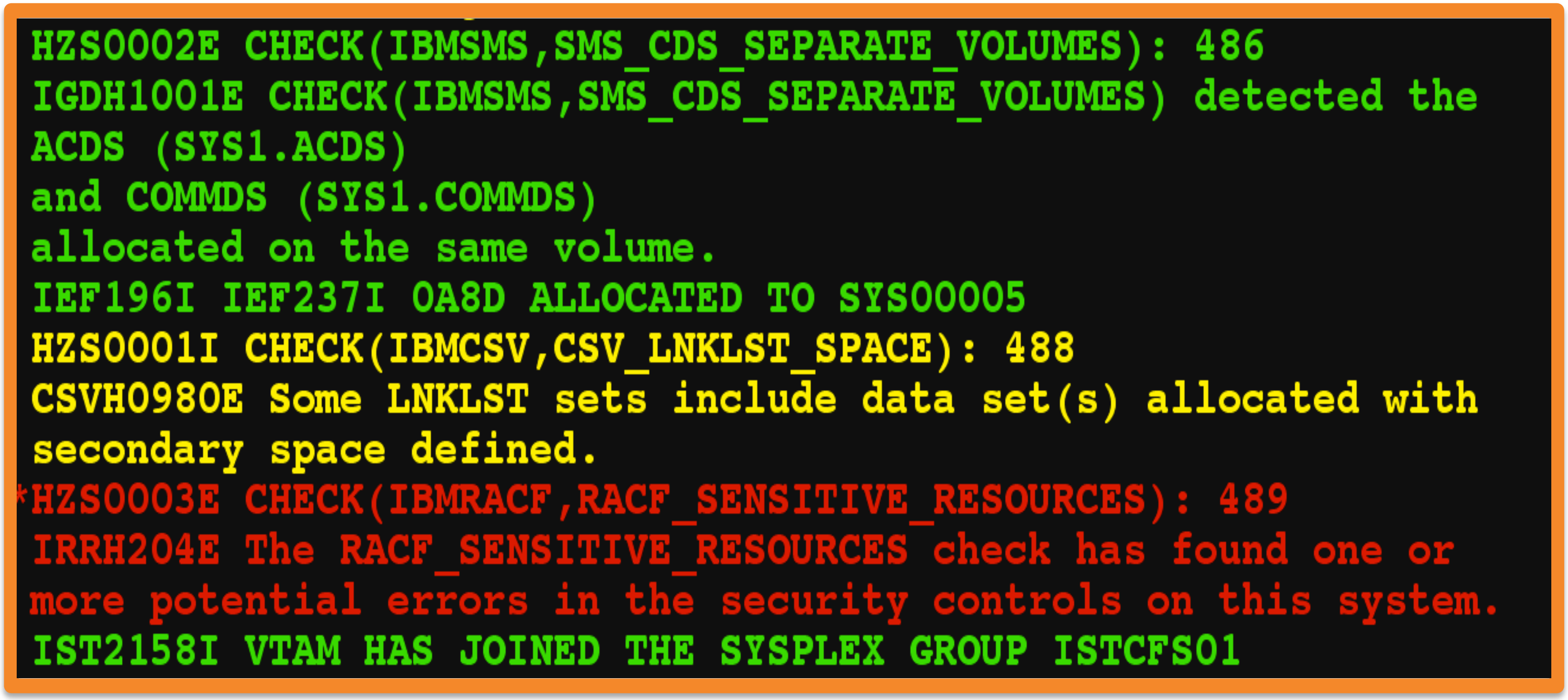
```
 HZS0002E CHECK(IBMXCF,XCF_CDS_SEPARATION): 969
 IXCH0240E Primary couple data sets for performance-sensitive types
 reside on the same volume.
*HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF): 970
 IXCH0242E One or more couple data sets have a single point of failure.
 HZS0002E CHECK(IBMXCF,XCF_CF_MEMORY_UTILIZATION): 971
 IXCH0456E Coupling facility memory utilization for one or more
 coupling facilities in use by the local system exceeds
 the owner defined maximum memory utilization
 of 60 percent.
 F HZSPROC,DISPLAY CHECK(IBMCNZ,CNZ_AMRF_EVENTUAL_ACTION_MSGS),
 POLICYEXCEPTIONS
 HZS0200I 07.31.41 CHECK SUMMARY     973
    THERE ARE NO CHECKS THAT MEET THE SPECIFIED CRITERIA
```

[1] *zZS18 – The Latest in IBM Health Checker for z/OS - Marna Walle, IBM Corporation*

[2] *Mark Nelson, z/OS Security Server (RACF) Design and Development*

Legacy Security?

The Future of Security > Health Checker > A Security Necessity



```
HZS0002E CHECK(IBMSMS,SMS_CDS_SEPARATE_VOLUMES): 486
IGDH1001E CHECK(IBMSMS,SMS_CDS_SEPARATE_VOLUMES) detected the
ACDS (SYS1.ACDS)
and COMMDS (SYS1.COMMDS)
allocated on the same volume.
IEF196I IEF237I 0A8D ALLOCATED TO SYS00005
HZS0001I CHECK(IBMCSV,CSV_LNKLST_SPACE): 488
CSVH0980E Some LNKLST sets include data set(s) allocated with
secondary space defined.
*HZS0003E CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES): 489
IRRH204E The RACF_SENSITIVE_RESOURCES check has found one or
more potential errors in the security controls on this system.
IST2158I VTAM HAS JOINED THE SYSPLEX GROUP ISTCFS01
```

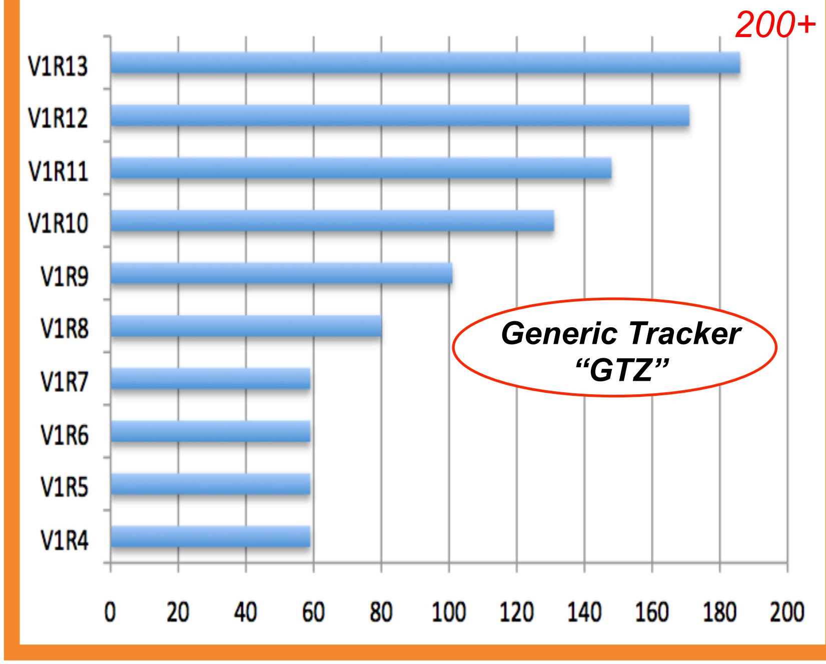
[1] *zZS18 – The Latest in IBM Health Checker for z/OS - Marna Walle, IBM Corporation*

[2] *NY/RACF – z/OS V2.1 RACF Update - Mark Nelson, z/OS Security Development, IBM*

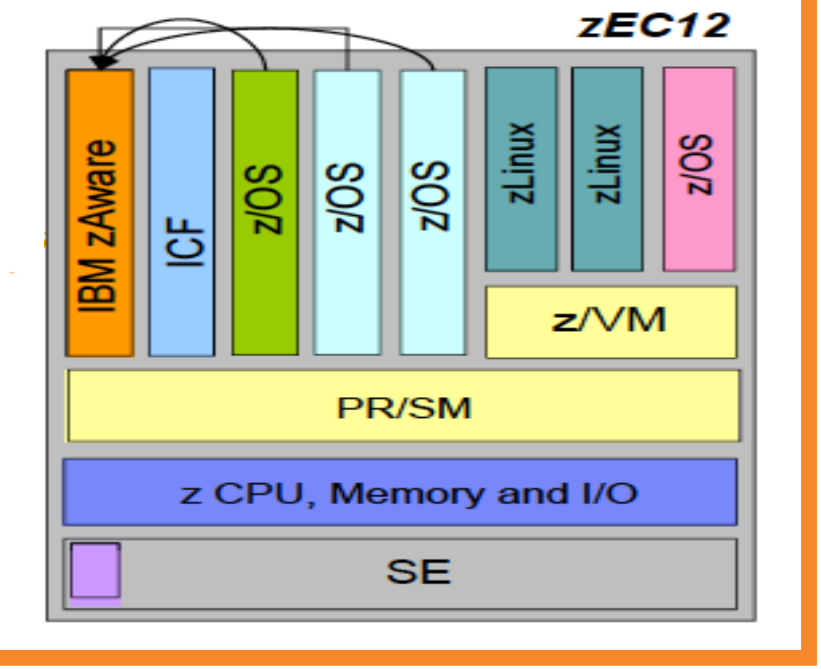
Legacy Security?

The Future of Security > Health Checker > A Security Necessity

IBM Health Checks for z/OS – The Check Inventory[1]



IBM zAware[2]

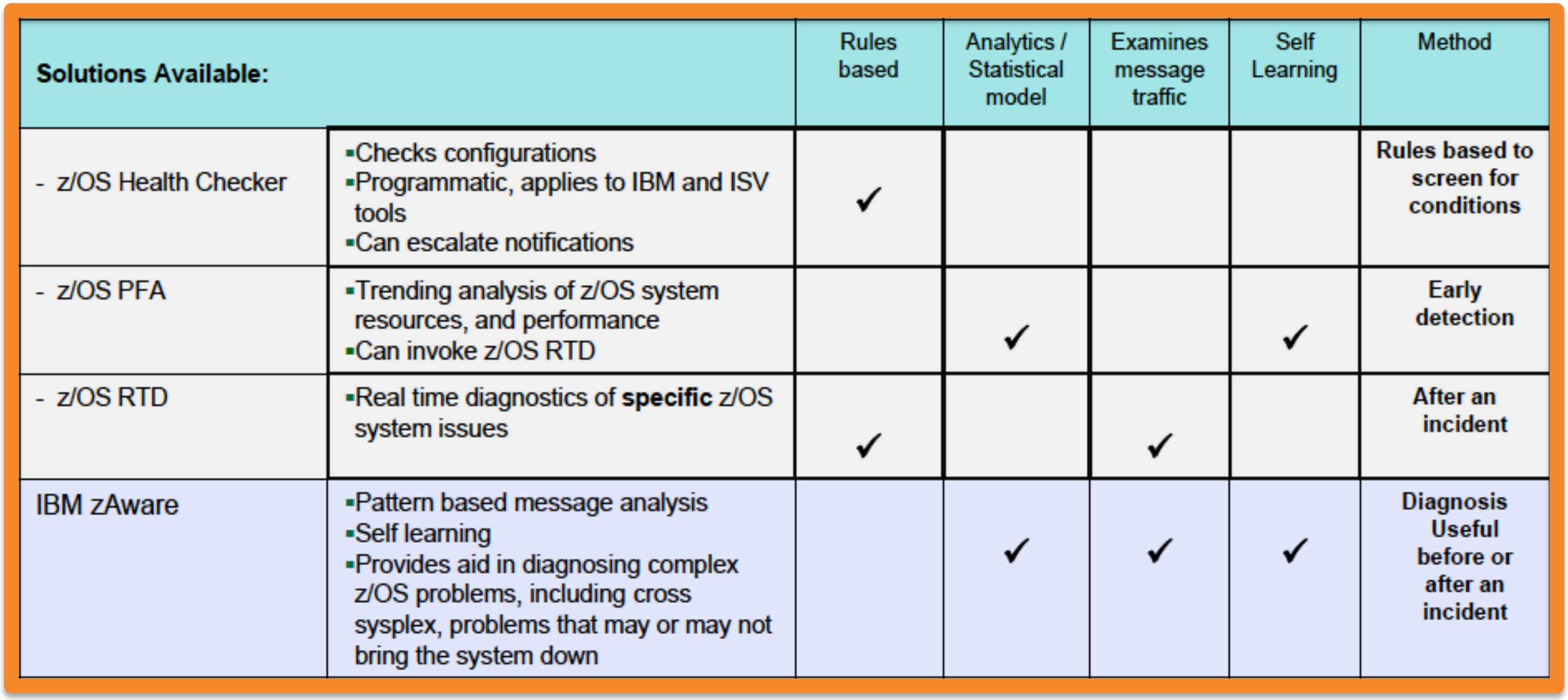


[1] *zZS18 – The Latest in IBM Health Checker for z/OS - Marna Walle, IBM Corporation*

[2] *SHARE SFO - 13063: IBM zAware - Using Analytics to Improve System z Availability - Garth Godfrey IBM Corporation*

Legacy Security?

The Future of Security > Predictive Analytics > Competing Strategies



Solutions Available:		Rules based	Analytics / Statistical model	Examines message traffic	Self Learning	Method
- z/OS Health Checker	▪Checks configurations ▪Programmatic, applies to IBM and ISV tools ▪Can escalate notifications	✓				**Rules based to screen for conditions**
- z/OS PFA	▪Trending analysis of z/OS system resources, and performance ▪Can invoke z/OS RTD		✓		✓	**Early detection**
- z/OS RTD	▪Real time diagnostics of **specific** z/OS system issues	✓		✓		**After an incident**
IBM zAware	▪Pattern based message analysis ▪Self learning ▪Provides aid in diagnosing complex z/OS problems, including cross sysplex, problems that may or may not bring the system down		✓	✓	✓	**Diagnosis Useful before or after an incident**

[1] *z/U 05/2013 - zZS21: Smart Monitoring of z/OS with IBM zAware by Riaz Ahmad, IBM Corporation*

Legacy Security?

The Future of Security > Your New Best Friend > The Boss!

For all its remarkable advances,
computation in the past half-century

—the era of “programmable” computers
—

has been limited to “yes/no” decisions.
The new era now emerging will unlock
far deeper understanding of the
complexities and ambiguities of the real
world

—both natural and man-made—

Source: IBM 2012 Annual Report - http://www.ibm.com/annualreport/2012/ - Published March, 2013

Legacy Security?

The Future of Security > The Real Threat > It's all up to you now!

"…our only limitation is the ability of our customers and prospects to grasp, understand and productively utilize the services, technology and product we provide…"

Source: Buck Rogers - VP Global Marketing, IBM Corporation, Executive Briefing
OMNI Hotel, Miami, FL - August, 1984 - More or Less its been long time!

That’s it folks, all done!

Session Evaluation - Session Number - 14228

Why Legacy Security Isn't Enough

Monday, August 12 at 11:00 am
Hynes Convention Center Room 207

Paul R. Robichaux
prr@newera.com

SHARE.org/BostonEval

QR Code

Visit www.SHARE-SEC.com
for more information on
the SHARE Security &
Compliance Project